Cabinet

SOUTH KESTEVEN DISTRICT COUNCIL

Tuesday, 18 May 2021 at 2.00 pm
Council Chamber - South Kesteven House, St. Peter's Hill, Grantham. NG31 6PZ

Cabinet Members:	Councillor Kelham Cooke, The Leader of the Council (Chairman) Councillor Barry Dobson, The Deputy Leader of the Council (Vice-Chairman) Councillor Annie Mason, Cabinet Member for Communities Councillor Dr Peter Moseley, Cabinet Member for Commercial and Operations Councillor Robert Reid, Cabinet Member for Housing and Planning Councillor Adam Stokes, Cabinet Member for Finance and Resources Councillor Rosemary Trollope-Bellew, Cabinet Member for Culture and Visitor Economy

Agenda

1. **Register of attendance and apologies for absence**

2. **Minutes of the previous meeting** (Pages 3 - 6)
   Minutes of the meeting held on 16 March 2021.

3. **Disclosure of Interests (if any)**

Items for recommendation to Council

4. **LeisureSK Ltd Management Fee** (Pages 7 - 11)
   Report from the Deputy Leader of the Council.

Items for Cabinet Decision: Key

5. **Pilot of Private Rented Sector Insurance Scheme for Lincolnshire** (Pages 13 - 19)
   Report of the Cabinet Member for Housing and Planning.

   Appendix 1 of this report is exempt under paragraphs 3 and 5, Schedule 12A of the Local Government Act 1972 (as amended).

Published and despatched by democracy@southkesteven.gov.uk on Monday, 10 May 2021.
01476 406080
Karen Bradford, Chief Executive
www.southkesteven.gov.uk

6. **Procurement of Improvement Works to HRA Properties to include Off Gas Heating Solutions** (To follow)
   Report of the Cabinet Member for Housing and Planning.

7. **Options for SK Legal Services** (Pages 21 - 25)
   Report of the Leader of the Council.

Items for Cabinet Decision: Non-Key

8. **Review of Data Protection Policies** (Pages 27 - 116)
   Report from the Leader of the Council.

Items for information

9. **Key and Non-Key Decisions taken under Delegated Powers** (Pages 117 - 129)
   Report from the Leader of the Council.

10. **Representations and questions from Non-Cabinet Members**

11. **Cabinet Forward Plan 1 June 2021 to 31 May 2022** (Pages 131 - 136)
    Report from the Leader of the Council.

Urgent Items

Items which the Leader is of the opinion should be considered at the meeting as a matter of urgency pursuant to Section 100(b)(4)(b) of the Local Government Act 1972 by reason of special circumstances.

Exempt Items

Under Section 100(a)(4) of the Local Government Act 1972, the press and public may be excluded from the meeting during any listed items of business, on the grounds that if they were to be present, exempt information could be disclosed to them as defined in the relevant paragraphs of Schedule 12A of the Act.

Minutes

Cabinet
Tuesday, 16 March 2021

SOUTH KESTEVEN DISTRICT COUNCIL

The Leader: Councillor Kelham Cooke, The Leader of the Council (Chairman)
The Deputy Leader: Councillor Barry Dobson, The Deputy Leader of the Council (Vice-Chairman)

Cabinet Members present

Councillor Annie Mason, Cabinet Member for Communities
Councillor Dr Peter Moseley, Cabinet Member for Commercial and Operations
Councillor Robert Reid, Cabinet Member for Housing and Planning
Councillor Adam Stokes, Cabinet Member for Finance and Resources
Councillor Rosemary Trollope-Bellew, Cabinet Member for Culture and Visitor Economy

Non-Cabinet Member present

Councillor Phil Dilks

Officers
Chief Executive (Karen Bradford)
Assistant Chief Executive, Housing Delivery (Ken Lyon)
Interim Director of Finance/Section 151 Officer (Richard Wyles)
Strategic Director Commercial and Operations (Gary Smith)
Interim Assistant Director of Housing (Chris Stratford)
Director of Law and Governance (Shahin Ismail)
Acting Principal Democratic Officer (Shelley Thirkell)
Democratic Officer (Lucy Bonshor)

76. Register of attendance and apologies for absence

All Cabinet Members were present.

The Leader referred to the budget that had been set at the beginning of March 2021. All vital front line services would continue to be delivered with no service reductions, together with implementing the ambitions outlined within the Council's Corporate Plan.

The Government's 'Road Map' out of lockdown was underway and direct support was being given to communities in South Kesteven and preparations were under way in relation to the economy. The business community continued to be supported with over £40m of business grants allocated to local businesses in South Kesteven.

Vulnerable residents were still being supported through the hardship fund and the Community Hub.

The result of the final submission in respect of the Future High Street Fund for Grantham Town Centre and High Street in the sum of £5.56m was still awaited. The bid for £950,370 of funding from the Public Sector Decarbonisation Scheme had been successful and LeisureSK Ltd had been successful in receiving £330,000 of funding from Sport England National Leisure Recovery Fund towards the cost of reopening the leisure centres in the District.

77. Minutes of the previous meeting

The minutes of the meeting held on 2 March 2021 were agreed as a correct record of the decisions taken, subject to the typographically error (none), against Councillor Ray Wootten's name being removed.

78. Disclosure of Interests (if any)

None disclosed.

79. Procurement of Improvement Works to HRA Properties

The Cabinet Member for Housing and Planning presented the report on the awarding of a contract for extensive refurbishment, structural and conversion works to Council properties. It was anticipated that this would only apply to a small number of properties. The current contract had lapsed and a new contract needed to be in place as soon as possible to allow for structural issues to be addressed. Tenants who were impacted would be fully consulted and the budget for the work had been previously approved.

The contract had been awarded under the Efficiency East Midlands Framework and was in accordance with the Council's Contract and Procurement Procedures.

On being put to the vote, it was **AGREED**:

To approve UK Gas Services Ltd (Building Services Division as the preferred contractor under the Efficiency East Midlands Framework) for the property improvement lot 3, at a total cost of £500,000 over the full five year term of the contract for the refurbishment/structural works to Council owned properties.

80. Procurement of Electrical Works

The Cabinet Member for Housing and Planning presented the report to award the Electrical Works Contract including electrical testing, electrical rewires and smoke detection upgrades to UK Gas Services Ltd. It was a significant contract which included the electrical certification to Council properties which was a critical requirement of the Council's compliance notice. It covered all Council stock, currently it was thought that only 50% of the Council's stock had electrical certification.

The contract had been awarded through the Efficiency East Midlands Framework and was fully compliant with the Council's procurement procedures. The budget to cover planned works and certification were provided for within the HRA Capital and Revenue expenditure budgets. The work would lift the safety and compliance of the Council's stock to meet the required Homes Standard.

The Leader stated that this was a positive step forward. The contractor provided the best value for money and also had the necessary resources to carry out the inspection works on behalf of the Council.

On being put to the vote, it was **AGREED:**

To approve the awarding of a contract to UK Gas Service Ltd in order to undertake electrical and smoke alarm testing including remedial and rewiring works for a two year period (with a potential 1+1+1 year extension) for a maximum total value of £3.050m.

81. Lincolnshire Homes for Independence Blueprint

The Cabinet Member for Housing and Planning presented the report which provided a draft blueprint for the provision of a greater range of housing options for those who needed additional support, and better integrated services between housing and health services to promote and sustain independent living.

The document overarched, housing, planning and community and related to the needs and opportunities for housing people whether that was in care, helping people remain in their own homes for longer through the granting of a Disabled Facilities Grant (DFG) or moving to more suitable accommodation. The Blueprint supported the ongoing partnership working of the Housing Health and Care Delivery Group across Lincolnshire.

Support was expressed by Cabinet to endorse the document.

On being put to the vote, it was **AGREED:**

To endorse the Lincolnshire homes for Independence Blueprint and works with partners to support the development of the delivery plan.

82. Matters Referred to Cabinet by the Council or Overview and Scrutiny Committees

The Leader stated that there was nothing to report since the last meeting of Cabinet on 2 March 2021.

83. Key and Non-Key Decisions taken under Delegated Powers

The Leader stated that there was nothing to report since the last meeting of Cabinet on 2 March 2021.

84. Representations and questions from Non-Cabinet Members

A Non-Cabinet Member welcomed the contract in respect of the electrical rewiring and asked whether the contract had lapsed or whether the previous contractor had failed to deliver the contract. The Interim Assistant Director of Housing replied that the contract had lapse and it was necessary to get a contractor in place to carry-out the electrical contract together with the required certification to comply with the compliance notice.

85. Cabinet Forward Plan 1 May 2021 to 30 April 2022

Cabinet noted the Forward Plan for the period 1 May 2021 to 30 April 2022.

86. Exclusion of Press and Public

It was proposed, seconded and agreed to exclude the press and public from the meeting, in accordance with Section 100A(4) of the Local Government Act 1972 (as amended) during consideration of the following item of business because of the likelihood that otherwise exempt information, as described in paragraph 3 of the Act would be disclosed to them.

87. Acquisition of Land in South Kesteven

The Cabinet Member for Commercial and Operations presented the exempt report on the acquisition of land in South Kesteven.

On being put to the vote, it was **AGREED** to approve the recommendations as contained within the exempt report from the Cabinet Member for Commercial and Operations submitted to Cabinet on 16 March 2021.

The report and associated appendices contain exempt information under paragraph 3 of Schedule 12A of the Local Government Act 1972 (as amended), due to the commercial sensitivity of the information contained therein.

SOUTH KESTEVEN DISTRICT COUNCIL

Cabinet

18 May 2021

Report of: Councillor Barry Dobson
The Deputy Leader of the Council

LeisureSK Ltd Management Fee

As a result of the ongoing impact of Covid-19 on the operation of LeisureSK Ltd, and the changes to business rates announced in the Budget in March 2021, Cabinet is requested to approve an increase in the budget allocation previously agreed to support LeisureSK Ltd for the financial year 2021/22. Cabinet is also invited to accept grant funding from Sport England.

Report Author

Karen Whitfield, Head of Leisure

01476 406239

karen.whitfield@southkesteven.gov.uk

Corporate Priority:	Decision type:	Wards:
Healthy and Strong Communities	**Budget and Policy Framework**	**Two or more Wards**

Reviewed by:	Nicola McCoy-Brown, Director of Growth and Culture	10 May 2021
Approved by:	Karen Bradford, Chief Executive	10 May 2021
Signed off by:	Councillor Barry Dobson, The Deputy Leader of the Council	10 May 2021

Recommendation (s) to the decision maker (s)

It is recommended that Cabinet:

1. **Accepts the award of grant funding from Sport England in the sum of £320,597 in order to support the reopening of the leisure facilities.**
2. **Agrees that the additional funding should be provided to LeisureSK Ltd to fund the business rates liability of £148,000 for financial year 2021/22.**

3. **Agrees to increase the budget allocation of £500,000 by an additional £108,125 making a total maximum budget allocation of £608,125.**

4. **Delegates authority to the Director of Growth and Culture, in consultation with the S151 Officer to determine the final amount of management fee payment due to LeisureSK Ltd subject to a full reconciliation of the income and expenditure of the company.**

1 The Background to the Report

1.1 Prior to the establishment of LeisureSK Ltd the Council developed a five-year trading forecast which included projected income and expenditure budgets for the district's leisure facilities. This work identified the level of management fee likely to be required by LeisureSK Ltd for the period January 2021 to December 2021 to be circa £500,000.

1.2 Subsequently, at a meeting of the Council held on the 26 November 2020, it was agreed that a budget not exceeding £500,000 would be provided to support the management fee required by LeisureSK Ltd. Delegated authority was provided to the Chief Executive of the Council, in consultation with the S151 Officer, to agree the final amount, noting that the payment would be subject to a full reconciliation to show the impact that Covid-19 had on income and expenditure.

1.3 The Annual Budget report presented to a meeting of the Council on the 1 March 2021 provided an update in relation to LeisureSK Ltd as the centres had not been able to open as anticipated on the 4 January 2021 due to the extension of lockdown measures in place. Therefore, the business plan was being reviewed and it was expected that the approved £500,000 management fee would need to be amended.

1.4 To ensure that any future budget requirement can be agreed as part of the Council's annual budget setting process it has been necessary to extend the first year of trading for LeisureSK Ltd to a period of fifteen months to include the period January 2021 to March 2022.

1.5 LeisureSK Ltd officially took over the management of the Council's leisure facilities from the 1 January 2021 however, in line with the lifting of restrictions, the centres remained closed until the 12 April 2021.

1.6 Whilst the centres remained closed the Directors of LeisureSK Ltd ensured that steps were taken to mitigate the financial impact of the extended closure. This included the appropriate use of the furlough scheme for the majority of the employees, whilst a small core of key operational staff were retained in order to undertake necessary health and safety and operational building checks.

1.7 During the time the centres were closed, opportunities to attract income have been severely limited. However, LeisureSK Ltd has been able to offset a number of costs from a hire fee obtained from renting out the table tennis centre at Grantham Meres Leisure Centre to the local Clinical Commissioning Group (CCG). This centre continues to operate as one of the main vaccination sites for Lincolnshire and, in addition to the hire fee received, LeisureSK Ltd have also been able to recharge other associated costs. Since the centres have re-opened, the hire fee has been increased to include loss of income.

1.8 The original budget allocation for the management fee payable to LeisureSK Ltd was based on the centres being operational from 4 January, albeit with social distancing measures still in place. Due to the delay in opening the facilities and the increase of the first trading period

to fifteen months it has been necessary to undertake a review of the management fee required.

1.9 The Council commissioned Sport and Leisure Consultancy Ltd to undertake a review of the first year of trading for LeisureSK Ltd utilising intelligence from the leisure industry on how the leisure centres were expected to recover once they reopened.

1.10 As a result of this work, it has been identified that the level of management fee required to support LeisureSK Ltd for the fifteen month period January 2021 to March 2022 is likely to be £780,722.

1.11 In December 2020 Sport England launched the National Leisure Recovery Fund. The fund totalled £100 million and was established by the Department of Culture Media and Sport (DCMS) to support the reopening of public sector leisure facilities following the national lockdown.

1.12 As part of the application process the Council were required to submit a detailed recovery plan on how the leisure centres would be re-opened and the level of activities to be offered. This included a detailed income and expenditure projection.

1.13 As a result of a successful application the Council have been awarded a total of £320,597 from the fund. As part of the accompanying grant funding conditions the grant may only be used to offset the expenditure as detailed within the recovery plan which was submitted as part of the application. This award will reduce the amount of support LeisureSK Ltd will require from the Council in the current financial year.

1.14 In addition to this it has been necessary to reassess the business rate liability for LeisureSK Ltd. When the Council established LeisureSK Ltd it received advice on the optimal company structure which would allow the company to take advantage of tax and business rate savings. As a result of this advice, it was originally envisaged that the company would apply to the Council for 100% discretionary business rate relief on the basis that the company was not for profit and was engaged in the delivery of leisure and physical activity within the district.

1.15 The budget in March 2021 provided an extension of the business rates holiday for the leisure centres until the end of June, after which time the rates liability will be discounted to one-third. If LeisureSK Ltd were liable for the full business rates liability, in the current year this would be £580,000, however considering the measures announced in the budget this reduces the liability to £148,000.

1.16 The Council's S151 Officer has undertaken financial modelling to establish the impact of the reduced business rates liability and determine the most financially advantageous outcome for the Council. This has concluded that the optimum scenario for 2021/22 will be for Leisure SK Ltd not to apply for discretionary relief and therefore to be liable for the payment of £148,000. This will need to be reflected in the management fee that the Council will pay for the financial year.

1.17 The revised management fee payment required by LeisureSK Ltd to cover the period January 2021 to March 2022 has been revisited to reflect the receipt of grant funding from Sport England and the additional business rates liability. This has resulted in a projected management fee payment of £608,125 being required.

1.18 Cabinet is therefore requested to approve a budget amendment of £108,125 to increase the previously allocated budget to £608,125 for the current financial year.

2 Consultation and Feedback Received, Including Overview and Scrutiny

2.1 Companies Committee have previously considered and endorsed the establishment of LeisureSK Ltd at the meetings held on the 22 September 2020 and 21 October 2020.

2.2 At the meeting of Companies Committee held on the 21 October 2020 it was recommended that a detailed Business Plan would be presented by the Directors of LeisureSK Ltd to Companies Committee at the earliest opportunity once the company had been fully established and the Directors had been appointed.

2.3 The Business Plan for LeisureSK Ltd was subsequently presented and approved at a meeting of Companies Committee on the 23 February 2021. The Business Plan included the increased management fee requirement of £780,722 to cover the impact of the lockdown and the extension of the first year of trading to a fifteen-month period.

2.4 At a meeting of the Council of the 1 March 2021 a budget allocation of £500,000 was proposed to support LeisureSK Ltd. However, it was noted within the report that this sum was being reviewed as the leisure centres remained closed as part of the national lockdown measures.

2.5 The Board of Directors of LeisureSK Ltd have fully considered the impact of the receipt of the grant funding from Sport England and the payment of the residual business rates liability. They remain committed to limiting the Council's financial exposure by controlling costs and maximising income opportunities to ensure LeisureSK Ltd represents value for money.

3 Available Options Considered

3.1 The recommendations within this report will result in the optimum financial outcome for the Council.

3.2 One of the main drivers for the establishment of LeisureSK Ltd was to secure the ongoing provision of leisure across the district. Without the requested increase in support LeisureSK Ltd will suffer cashflow problems and may need to cease trading, resulting in the loss of leisure provision across the District.

4 Preferred Option

The preferred option is for Cabinet to approve the acceptance of the award of grant funding the Council has received from Sport England in the sum of £320,597 and agree to the payment of the residual business rates liability for LeisureSK Ltd for the financial year 2021/22 in the sum of £148,000. This will result in an additional budget allocation of £108,125 being required to support LeisureSK Ltd for the fifteen-month period January 2021 to March 2022.

5 Reasons for the Recommendation (s)

5.1 The recommendations within this report will provide a budget framework to support LeisureSK Ltd in its first year of operation, and also ensure that any final payment due is limited to the operational deficit of the company.

6 Next Steps – Communication and Implementation of the Decision

6.1 Should the additional budget allocation be approved a detailed breakdown of income and expenditure targets will be confirmed to the Board of Directors for LeisureSK Ltd. These targets will form part of a monthly budget review at Board meetings.

It is the role of the Directors for LeisureSK Ltd to ensure that the company is operated on a sound financial basis and that the company achieves the financial targets agreed, limiting any financial burden on the Council.

7 Financial Implications

7.1 The proposed management fee payable by the Council for the period 1 January 2021 – 31 March 2022 is calculated by:

Management fee	£780,722
Leisure recovery funding	(£320,597)
Business Rate payable	£148,000
Net fee payable	£608,125

7.2 This represents an increase of £108,125 from the funding level approved by Council on 26 November 2020 although the management fee period has been extended by 3 months in order to align the trading year to match the Council's financial year. The funding level for 2022/23 will be considered once the business plan has been updated and a formal proposal has been put for the Council to consider.

Financial Implications reviewed by: Richard Wyles, Interim Director of Finance

8 Legal and Governance Implications

8.1 The Council's Financial Regulations provide that Cabinet can approve additions to the budget framework up to £150,000 per addition and up to £500,000 cumulative per financial year. The requested increase is therefore within Cabinet's approval limits.

Legal Implications reviewed by: Shahin Ismail, AD Law and Governance

9 Equality and Safeguarding Implications

9.1 None arising from this report.

10 Risk and Mitigation

10.1 The Directors of LeisureSK Ltd have developed a Risk Register for the company to ensure that any existing or emerging risks are identified, and mitigating actions are in place.

11 Community Safety Implications

11.1 None arising from this report.

12 How will the recommendations support South Kesteven District Council's declaration of a climate emergency?

There are no carbon footprint implications as a result of this report.

Report Timeline:	Date of Publication on Forward Plan (if required)	19 April 2021
	Previously Considered by: Not applicable	Not applicable
	Final Decision date	18 May 2021

This page is intentionally left blank

SOUTH KESTEVEN DISTRICT COUNCIL

Cabinet

18 May 2021

Report of: Councillor Robert Reid

Cabinet Member for Housing and Planning

Pilot Private Rented Sector Insurance Scheme for Lincolnshire

This report seeks approval to undertake a pilot insurance scheme for guaranteed rent and property damage liability for private rented sector landlords, supporting the use of the private rented sector to meet housing demand within the District.

Appendix 1 of this report is exempt under paragraphs 3 and 5, Schedule 12A of the Local Government Act 1972 (as amended) because it contains the following:

- **Information relating to the financial or business affairs of any particular person (including the authority holding the information) refers to the policy cost breakdown that will be attached to individuals.**
- **Information in respect of which a claim to legal professional privilege could be maintained in legal proceedings – refers to the Service Level Agreement which received Legal Advice from South Holland District Council.**

Report Author

Celia Bown, Senior Housing Policy Officer

07900 270419

c.bown@southkesteven.gov.uk

Corporate Priority:	Decision type:	Wards:
Housing that meets the needs of all residents	**Key**	**All Wards**

Reviewed by:	Helen Clarke, Head of Housing	26 April 2021
Approved by:	Andrew Cotton, Director for Housing and Property	29 April 2021

Signed off by:	Councillor Robert Reid, Cabinet Member for Housing and Planning	30 April 2021

Recommendation (s) to the decision maker (s)

1. **Cabinet approves the introduction of a pilot insurance-backed rent guarantee and property damage liability scheme using the product developed by Help2Rent on the following basis:**
    a) **For a pilot period of no more than 12 months during 2021/22;**
    b) **That no more than 50 client referrals are made with a maximum expenditure of £29,200; and**
    c) **That a detailed report on the outcomes and value-for-money of the scheme is submitted for Cabinet's consideration at the conclusion of the pilot to determine if the scheme is continued.**
2. **Cabinet notes the funding for such a scheme will be provided through the Homelessness Prevention Grant awarded to the Council for the 2021/22 financial year.**

1 The Background to the Report

1.1 In common with most stock-retained local authorities, South Kesteven District Council cannot meet the housing demand within the district solely within its own housing stock. This is of importance given the Council's duties under the relevant homelessness legislation to provide accommodation and to discharge its homelessness prevention duties. The Localism Act 2011 provided a power to local authorities to discharge such duties into private sector rented accommodation.

1.2 There are, however, some difficulties in respect of nominating such clients into private rented accommodation, as landlords often seek additional guarantees, such as rent and property damage payment guarantees, from local councils associated with rent deposit schemes. The provision of such schemes has assisted local council nominations into private rented stock and South Kesteven District Council has used these mechanisms successfully for the past two years.

1.3 Changes to the welfare benefits system, including Local Housing Allowance and the introduction of Universal Credit (which has rent payment delays associated with claiming the benefit) has led to many private landlords being reluctant to take homeless households and other referrals from Councils. This is because these clients represent a rising and continued risk of failing to meet rent payments on a regular and sustainable basis. This means that inevitably people spend longer in Bed and Breakfast (B&B) or Temporary Accommodation (TA) before a placement or suitable property can be found in the local authority's own stock.

1.4 With these issues and challenges in mind, local councils nationally have been working on a potential means by which exposure to unpaid rent for landlords in the private sector could be reduced, specifically where a council nominates clients into private rented accommodation. It has been recognised for some time now that an insurance backed policy, to minimise risk, offers the best opportunity to address these matters.

1.5 More recently, a company called 'Help2Rent' has developed and piloted a product with a London council, which offers bespoke insurance policy cover, including Tenant's Liability Insurance and Landlord's Insurance, to cover losses from non-payment of rent and property damage. The scheme involves landlords being contacted, to inform them that the Council would be willing to nominate a client for housing and then pay for the insurance premiums (where the Council is discharging its homelessness duty to accommodate). This then covers the landlord for any loss of rent or property damage during the period of cover. This substantially mitigates the risks to the landlord and makes it more likely that the Council can successfully nominate qualifying clients into private rented properties. It is also likely to save potential costs associated with any B&B costs and reduce the need to pay monies in advance for a deposit or rent in advance. Appendix 1 sets out the product details.

1.6 Council officers have been working as part of a consortium of four authorities across Lincolnshire, with South Holland District Council acting as the lead contact with the Help2Rent Company to develop the product across the County. It has been recognised that the development of a service level agreement (SLA) will be the most effective way of developing an operational relationship with the company and this has now reached draft form for South Kesteven District Council officers to consider. This will, if the scheme is approved, form the basis of the working arrangements between the Council and Help2Rent. By signing the SLA, the Council is not tied into a minimum spend profile and it

is proposed that no more than 50 nominations to be made, to review all operational matters and the final cost benefit analysis of the product, before considering any longer-term arrangements.

1.7 The cost of each policy for 12 months' cover is set out in Appendix 1.

1.8 Based on a maximum 50 such arrangements for cover being put in place to cover the pilot period, it is estimated that maximum costs of circa £29,200 per annum would be incurred.

2 Consultation and Feedback Received, Including Overview and Scrutiny

2.1 This product is only available to local authorities and therefore nothing comparable is currently available in the wider market. The London Borough of Southwark have already piloted the policies and they noted that Help2Rent's insurance policies are a niche offering, that are considered to offer good value for money, and are currently the only one of its kind.

2.2 The Welland Procurement Partnership have advised that an exemption request can be made to enable the Council to undertake a pilot of the scheme, before concluding what longer-term procurement exercise might be appropriate.

2.3 No recommendations were made by the Rural and Communities Overview and Scrutiny Committee who consider the scheme at the 11th March 2021 meeting.

3 Available Options Considered

3.1 Option 1 - continue as at present

This would result in continued difficulties in housing people within the private rented market and would place increased pressure upon our housing register, Council housing stock and other social housing registered provider stock.

Option 2 – purchase of the Help2Rent insurance policies

Help2Rent's insurance policies are a niche offering, that are considered to offer good value for money. They have been designed and tested with specific local authority needs in mind.

4 Preferred Option

4.1 Option 2

5 Reasons for the Recommendation (s)

5.1 The quantity of available public sector stock does not meet the demand for housing and therefore, there is a reliance on private rented stock to meet some of this demand. To increase the number of available private rented housing options across the district, this insurance scheme for guaranteed rent and property damage liability is proposed.

6 Next Steps – Communication and Implementation of the Decision

6.1 Officers would liaise with South Holland District Council to understand how they generated landlord interest in this scheme across their district. If the scheme is approved, contact will be made with the private landlords within the District to discuss the scheme, how it works, and to explain the benefits that could exist if they participated with the Council. The

intention is to advertise the scheme, utilising social media and the South Kesteven landlord forum to present the product.

7 Financial Implications

7.1 The maximum costs associated with running a pilot scheme up to a maximum of 50 insurance backed referrals to private landlords would not exceed £29,200. The necessary funding would be provided from the Homelessness Prevention Grant awarded, totalling £335,841 to SKDC for the 21/22 financial year. It is important that there is a timely and robust review of this initiative to assess the effectiveness of the scheme against the stated objectives. Currently, there is no budget provision available beyond the financial year 2021/22.

Financial Implications reviewed by: Richard Wyles, Interim Director of Finance

8 Legal and Governance Implications

8.1 The scheme can lawfully be implemented and there are no further legal implications arising from the policy.

Legal Implications reviewed by: Shahin Ismail, Director of Law and Governance

9 Equality and Safeguarding Implications

9.1 In assessing and placing clients into housing as part of the Council's homelessness duties and responsibilities, the Council must apply the necessary Equality and Safeguarding regulations and good practice considerations. There will not be any differentiation made between people with the Equality Act 2010 protected characteristics and those without, when the insurance policies are purchased.

10 Risk and Mitigation

10.1 Very low risk as all terms and conditions of the insurance cover will be explained to the landlords before signing and agreeing to cover.

11 Community Safety Implications

11.1 All necessary individual and community safety considerations are assessed in determining a landlord's suitability to access the scheme and act as a nominated landlord used by the Council.

12 How will the recommendations support South Kesteven District Council's declaration of a climate emergency?

12.1 Neutral (no carbon impact)

13 Other Implications (where significant)

13.1 None known

14 Background Papers

14.1 Help2Rent presentation (confidential)

15 Appendices

15.1 Appendix 1 – Help2Rent insurance policy costs

Report Timeline:	Date of Publication on Forward Plan (if required)	19 April 2021
	Previously Considered by: Rural and Communities Overview and Scrutiny Committee	11 March 2021
	Final Decision date	18 May 2021

By virtue of paragraph(s) 3, 5 of Part 1 of Schedule 12A
of the Local Government Act 1972.

Document is Restricted

This page is intentionally left blank

SOUTH KESTEVEN DISTRICT COUNCIL

Cabinet

18 May 2021

Report of: Cllr Kelham Cooke

Leader of the Council

Options for SK Legal Services

A report seeking approval to join the Lincolnshire Legal Services Partnership (LSL) to access legal support and advice, whilst retaining a small 'legal client' function in house.

Report Author

Shahin Ismail, Assistant Director Law and Governance

Tel: 01476 406110

Email: s.ismail@southkesteven.gov.uk

Corporate Priority:	Decision type:	Wards:
A high performing Council	**Key**	**Two or more Wards**

Reviewed by:	Alan Robinson, Deputy Chief Executive	5 May 2021
Approved by:	Karen Bradford, Chief Executive	6 May 2021
Signed off by:	Cllr Kelham Cooke, Leader of the Council	10 May 2021

Recommendation (s) to the decision maker (s)

1. **Notes the content of the report.**
2. **Considers the options presented.**
3. **Approves the recommendation to join the established and successful Lincolnshire Legal Services Partnership, and retain the existing staff, as set out in Option 4.**

1 The Background to the Report

1.1 Over the last 10 years, the team has reduced in size due to a number of factors, including the ability to recruit and retain the right skills and experience. The service currently has two members of staff and carries two vacancies.

1.2 Management analysis, supported by financial data suggests that the requirements for legal support have in fact increased, as the Council's plans and ambitions have developed.

1.3 The newly adopted Corporate Plan places significant emphasis on strong robust decision making. The legal input into Council decision making is central, as a strong legal function should provide support to all directorates and to the Council's committees.

1.4 A modern and high performing Council requires a range of legal support, including corporate and commercial advice; procurement advice; committee support and governance law; judicial review; property law; enforcement and regulatory work; expertise in civil and criminal courts and specialist tribunals. This full range of expertise cannot be provided by a small in-house team.

1.5 Equally, the Council requires legal specialisms, including planning, housing, environmental health, companies' law, property law and governance law.

1.6 This paper details options to provide the Council with the legal support it needs, in a cost efficient and more coherent way.

2 Consultation and Feedback Received, Including Overview and Scrutiny

2.1 Consultation has taken place with the unions and with the legal staff. The council's Senior management Team has also been consulted.

2.2 Staff consultations were positive, as the preferred option sees both jobs retained. Senior Team recognised and welcomed the changes.

3 Available Options Considered

3.1 **Option 1: Fully outsource to Lincolnshire Legal Services (LSL)**

3.2 This would involve outsourcing the entire legal function to LSL, including transferring the existing staff under the TUPE Regulations into Lincolnshire County Council, which is the employer of all staff in the LSL partnership.

3.3 Lincolnshire Legal Service (LSL) provide a shared service function for most of the Lincolnshire authorities. The model is governed by a Partnership Board and users only pay for the service used. They have the size, scale and team expertise to provide a holistic service. Their hourly rates are low in comparison to other external firms of solicitors and whilst slightly higher than a direct in-house cost, their hourly rates factor in on costs. Any surplus income generated by the Partnership is shared among the partner councils.

3.4 A fully outsourced model would leave no legal staff inside the Council. This is not considered ideal, as there are day to day legal matters that it is more efficient to provide in house such as sealing of contracts, maintaining the deed store, attend at committees, and

assist members and officers in day to day queries. An in-house team would also act as the 'gateway' for procuring certain types of legal support, to ensure Council resources are used effectively.

3.5 **Option 2: No change**

3.6 The current model does not cater for all the Council's legal requirements. Capacity is very stretched and the in-house team cannot provide expertise in the full range of legal matters.

3.7 **Option 3: Build up a fully functioning in house team**

3.8 In order to provide the range of skills and expertise needed, we would need to recruit up to 5 additional lawyers. This will take up to 2 years to get the correct mix. There would be redundant capacity in the team, because our need for some expertise in each area of law is intermittent. It would be more efficient enter into a partnership to source this support.

3.9 **Option 4: Hybrid model**

3.10 This is the recommended option. This model would see LSL delivering the majority of the Council's legal support, while retaining a small in-house team. This model would ensure an optimal mix of legal support. LSL would provide certainty and the full range of skills, and as the Council would be a full partner, any surplus income would be recycled back to the Council as a partner.

3.11 LSL are highly regarded by the councils who use them. We have been utilising LSL's services on an informal arrangement over the past 12 months and our experience of their work has been universally positive to date. The advice is of a high quality, and very tight timescales have been met. The model is efficient as we would only pay for what we use.

3.12 There will be occasions when LSL have a conflict of interest with Lincolnshire County Council. This conflict is manageable, and the Solicitors Regulatory Authority requires arrangements to ensure client confidentiality is maintained in the event of a conflict. LSL have robust arrangements in place to manage conflicts and SKDC would use other external partners in the event of a conflict or for any sensitive issues.

3.13 The existing legal budget would be used in a targeted way, so that the right skills and expertise can be purchased as and when needed.

4 Preferred Option

4.1 Option 4 is the preferred and recommended option.

4.2 The partnership will be able to provide timely support on a wide range of legal issues which just would not be affordable for a District Council to maintain in an in-house team. The rates provide for best value and there is also the opportunity for SKDC to share any surplus that the partnership generates.

4.3 The retained in house team will act as 'intelligent client' and will be able to advise officers and members as to whether external legal support is required and will assist directorates to procure only that which is necessary. In this way, few can ensure financial controls are implemented on the use of LSL, the in-house team will act as a 'gateway' to determine when legal services can be procured from LSL.

5 Reasons for the Recommendation (s)

5.1 Joining the LSL shared service partnership will provide access to a holistic and comprehensive legal team who, through working in the County Council and with a majority of the Lincolnshire District Councils, have expertise that cannot be provided in a value for money fashion by an in-house team.

5.2 The current team has reduced in recent years and whilst they provide an excellent service, the breadth of requirements has become a challenge. A number of options have been explored, and financial analysis conducted to demonstrate that an outsourced option is commercially the most viable.

5.3 Whilst the legal function would be outsourced, the in house staff would remain employed in house, on the 'client' side, to ensure contracts and deeds are sealed and retained; to oversee s106 agreements; Tree Preservation Orders; right to buys; support committees; support in house project teams; provide support in the regulatory areas such as Freedom of Information and Subject Access; and provide corporate support to the Chief Executive and Deputy Chief Executive in governance and constitutional work.

6 Next Steps – Communication and Implementation of the Decision

6.1 LSL are taking a similar paper through their committees and are committed in principle to this proposal. Formal implementation can take place in June 2021.

7 Financial Implications

7.1 Option 4, if implemented, will require financial controls to be introduced in order to ensure that expenditure is controlled and managed. In 2020/21 external legal spend was £124,900. This cost was managed by utilising available budgets including the current staffing vacancies. The external legal spend has therefore been within the current budget for legal services. It will be important to ensure that the utilisation of the external legal service is kept within approved budget levels and so a centralised process is being developed to ensure legal service requests are managed and monitored.

7.2 By retaining the staff who can do some of the legal work such as the right to buy work will ensure costs are kept down.

Financial Implications reviewed by: Richard Wyles, Interim Director of Finance

8 Legal and Governance Implications

8.1 The Council will be entering into a partnership agreement, the terms of which are highly flexible and do not require exclusivity or any minimum level of spend. This provides flexibility for the Council in how it uses the services LSL. There is a Partnership Board on which the Council will have a seat. Joining a shared service arrangement is compliant with procurement law.

Legal Implications reviewed by: Alan Robinson, Deputy Chief Executive

9 Equality and Safeguarding Implications

9.1 No implications.

10 Risk and Mitigation

10.1 Neutral implications.

11 Community Safety Implications

11.1 None.

12 How will the recommendations support South Kesteven District Council's declaration of a climate emergency?

12.1 The changes will have a neutral impact on climate change, as much of the work will be done remotely.

13 Other Implications (where significant)

13.1 None.

14 Background Papers

14.1 None.

15 Appendices

15.1 None.

Report Timeline:	Date of Publication on Forward Plan (if required)	19 April 2021
	Previously Considered by:	Not applicable
	Final Decision date	18 May 2021

This page is intentionally left blank

SOUTH KESTEVEN DISTRICT COUNCIL

Cabinet

16 March 2021

Report of: Councillor Kelham Cooke
The Leader of the Council

Data Protection Policy review

This report is in response to an audit action to review all Data Protection policies annually.

Report Author

Stacy Carter, Data Protection Support Officer

Tel: 01476 406080 Ext: 6511

Email: Stacy.carter@southkesteven.gov.uk

Corporate Priority:	Decision type:	Wards:
High Performing	**Administrative**	**All Wards**

Reviewed by:	Shahin Ismail, Director of Law and Governance	04/03/2021
Approved by:	Karen Bradford, Chief Executive	10/05/2021
Signed off by:	Councillor Kelham Cooke, Leader of the Council	10/05/2021

Recommendation (s) to the decision maker (s)

That Cabinet approve the proposed updates and amendments to the existing Data Protection policies.

1 The Background to the Report

1.1 The existing SKDC Data Protection policies are subject to an annual review. The internal GDPR audit conducted in August 2020, identified that the existing policies had not been reviewed since 2018.

2 Consultation and Feedback Received, Including Overview and Scrutiny

2.1 There is no requirement for consultation for this year's review. There are no material changes that effect current ways of working or that will impact Council services.

3 Available Options Considered

3.1 The proposed changes for each policy are outlined below. Existing and reviewed policies can be found in the report folder at this location: *\\nassau\Global\Democratic\Reports\Cabinet\2020-21\11.16 March 2021\Data Protection Policies*

3.2 **Breach reporting form**

3.3 This form has been updated to align with ICO reporting requirements.

3.4 An additional question *'Do you consider the data to be contained and the risk to data subjects mitigated?'* has been added for reporting officers to complete.

3.5 All questions for the Data Protection Officer or Data Protection Support Officer to complete have been moved to the second half of the form.

3.6 **Data Protection policy**

3.7 The language has been changed to match current legislation eg. *PIA to DPIA and Sensitive to Special category data*.

3.8 Section 10 – Training point 10.1 has been replaced with 10.1 and 10.2

Previous

10.1 Data Protection training is important so that we can be sure that all employees and agency workers understand their responsibilities. All employees (including temporary employees) will complete Data Protection training every year and Elected Members will be offered the same training.

Replaced by

10.1 Staff training ensures the organisation is compliant with legislative requirements and provides employees with the knowledge of their responsibility to keep personal data secure.

10.2 All employees must complete Data Protection training annually (including temporary employees). Members will complete data protection awareness sessions at Member induction. They will also be offered Data Protection training within the Member Development Programme.

3.9 **Protocol for protection of personal data**

3.10 The language has been changed to match current legislation.

3.11 **Procedure for reporting breaches**

3.12 The language has been changed to match current legislation.

3.13 The breach reporting form has been removed from the policy this allows the form to be updated when required without requiring a policy review.

3.14 **Procedure for undertaking a Data Protection Impact Assessment (DPIA)**

3.15 The DPIA form has been removed from the policy this allows the form to be updated when required without requiring a policy review.

3.16 **Information Governance Guidance**

3.17 Section 2.2 – acknowledging that the council will be able explore the use of data when acting commercially.

Previous

Effective Information Governance enables the Council to safeguard personal information and to make the best use of the information that it holds.

Updated

Effective Information Governance enables the Council to safeguard personal information and to make the best use of the information that it holds. Acknowledging the ways, a council acting commercially may use and share data whist ensuring compliance with current data protection laws.

4 Preferred Option

If Cabinet agree with the proposed material changes and the vocabulary changes then the policies can be updated on the SKDC intranet.

5 Reasons for the Recommendation

5.1 Most of the proposed changes are non-material, they consist of vocabulary changes to bring the policies in line with current legislation and the removal of forms from policies.

5.2 The material changes are shown in 3.6 to 3.8 and contain changes to organisational training. The change includes references to data protection training as part of the Member Development Programme. This ensures organisational compliance with data protection legislation.

6 Next Steps – Communication and Implementation of the Decision

6.1 The Cabinet decision on this report will be made available through the usual democratic processes.

6.2 The reviewed policies will be placed on the SKDC intranet and an all staff email will inform employees of the updates and how to access them.

7 Financial Implications

7.1 There are no financial impacts.

Financial Implications reviewed by: Richard Wyles, Interim Director of Finance

8 Legal and Governance Implications

8.1 The proposed updates do not have any legal impacts.

8.2 The material change in 3.6 to 3.8 will require Members to attend a data protection training session.

8.3 SKDC 'commerciality' need to be considered and included within the policy review.

8.4 Version control and review dates must be added to the policy documents.

8.5 Reference to the SIRO post and responsibilities must remain within the policies.

Legal Implications reviewed by: Shahin Ismail, Director of Law and Governance

9 Equality and Safeguarding Implications

9.1 There are none.

10 Risk and Mitigation

10.1 If the proposed updates are not accepted, we may be open to non-compliance in respect of training.

11 Community Safety Implications

11.1 There are none.

12 How will the recommendations support South Kesteven District Council's declaration of a climate emergency?

12.1 There is no impact.

13 Other Implications (where significant)

13.1 None.

14 Appendices

14.1 Appendix 1 – Existing policies

14.2 Appendix 2 – Reviewed policies

Report Timeline:	Date of Publication on Forward Plan (if required)	2 February 2021
	Previously Considered by: Cabinet	N/A
	Final Decision date	16 March 2021

Appendix 1 – Breach Reporting Form			
Reporting Officer			
Team			
Service Area and name of Business Manager			
Date of Breach			
Date Breach discovered			
Date Reported to the ICO			
Please provide a brief explanation for any delay between the breach being discovered and the ICO being notified			
Does the breach involve sensitive / special category personal data?	YES	NO	Unknown at time of reporting
Does the breach involve card data?	YES	NO	Unknown at time of reporting
A description of the breach – what caused it, what data was affected, what was / could be the impact of the breach?			

To be completed by the Data Protection Officer			
Risk Assessment?	**HIGH**	**MEDIUM**	**LOW**
Reported to the ICO?	**YES**	**NO**	
Date reported to the ICO			

If ICO not notified, record the reason why		
Data subjects informed?	**YES**	**NO**
Date data subjects informed		
If data subjects not informed, record the reason why		
Describe the steps taken to remedy the breach / recover the data or to mitigate the risk and impact of the breach		
Post breach analysis, follow up actions and lessons learnt		

This page is intentionally left blank

South Kesteven District Council

Data Protection Policy

June 2018

CONTENTS

1 Introduction

1.1 This is South Kesteven District Council's Data Protection Policy.

1.2 South Kesteven District Council processes personal data to carry out its duties and obligations. This policy sets out the Council's commitment to protecting and handling personal data.

2 Scope

2.1 This Policy applies to:

- All employees of the Council;
- Members of the Council;
- Suppliers and Contractors of the Council;
- Temporary staff engaged by the Council;
- Volunteers at the Council;
- Others using the Council's information or systems

2.2 Some of the Council's obligations in this policy are supported by other policies and procedures, where relevant, links to those policies and procedures are provided in this document.

2.3 This policy relates to personal data, which means any information in paper or digital format relating to a person who can be identified by that information. Personal data may also be classed as special category (sensitive) data. The definitions of personal and special category (sensitive) data are attached at Appendix 1.

3 Data Protection Principles

3.1 South Kesteven District Council must protect and process the personal data, which it holds in accordance with data protection principles established by law. The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR), require us to be sure that all personal data is:

- Processed fairly, lawfully and in a transparent manner ('lawfulness, fairness and transparency');

- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');

- Adequate, relevant and limited only to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- Accurate and where necessary kept up to date, erased or rectified without delay ('accuracy');

- Kept in a form which permits identification of data subjects for no longer than is necessary ('storage limitation');

- Processed in accordance with the rights of data subjects

- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4 General requirements

4.1 The main requirements for data protection are that:

- Personal data will only be accessed by those who need it for work purposes
- Personal data will not be divulged or discussed except when performing normal work duties
- Personal data must be kept safe and secure at all times, including at the office, public areas or in transit
- Personal data will be regularly reviewed and updated
- Internal and external queries about data protection to the Council must be dealt with effectively and promptly

How the Council complies with these requirements is set out in the IT Security Policy http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=24180&p=0

Acceptable Use of IT Policy
http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=24181&p=0

and the Protocol relating to the protection of personal data
www.southkesteven.gov.uk/CHttpHandler.ashx?id=24183&p=0

5 Information Sharing

5.1 Personal data may need to be shared with other organisations in order to deliver our services or perform our duties. This can only be done where we have permission or if there is a legal obligation for us to share personal data.

5.2 Where the Council regularly shares personal information with our partners and other organisations an Information Sharing Agreement will be put in place. This agreement is signed by all partners to the sharing and agrees a set of standards and best practice surrounding Data Protection. However, these are not needed when information is shared in one-off circumstances but a record of the decision and reasons for sharing information will be kept.

5.3 All Data Sharing Agreements will be registered with the Council's Data Protection Officer. That officer will maintain a register of all our Data Sharing Agreements.

5.4 Where we give personal data or give access to personal data that we hold to anybody acting on behalf of the Council, we will require that party to sign a Non-Disclosure Agreement.

6 Privacy Impact Assessments (PIAs)

6.1 PIAs will be completed to help identify and minimise risks to the protection of data in the following situations where personal data is held by the Council:

- At the beginning of a new project or when implementing a new system
- Before entering a data sharing agreement
- When major changes are introduced into a system or process

For further guidance on undertaking Data Protection Impact Assessments (PIA's), please read our Procedure for Undertaking a Data Protection Impact Assessment www.southkesteven.gov.uk/CHttpHandler.ashx?id=24187&p=0

7 Data Subject Rights

7.1 The Council is committed to ensuring individuals can freely exercise their rights. Below is a summary of those rights.

- **Right to Access**

  This allows the individual to ask the Council if it holds personal information about them, what it uses the information for and to be given a copy of that information.

  Anyone wanting to know what personal data the Council holds about them can make a Subject Access Request by completing "Subject Access Information Request Form". This form and the

procedure for making applications and dealing with SAR's is available on this link:
http://www.southkesteven.gov.uk/index.aspx?articleid=8460

- **Right to correct incorrect information (rectification)**

This means the right to have your personal data corrected if the data we hold is not correct, or completed if it is incomplete. A request for a correction must be made in writing to the Data Protection Officer with proof of identity.

- **Right to erasure**

This means you have a 'right to be forgotten' and all your personal data deleted in certain circumstances. A request for erasure must be made in writing to the Data Protection Officer with proof of identity.

- **Right to restriction of processing of personal data in certain circumstances.**

This means that you can ask us to limit the way that we use your personal data in some situations. A request for restriction must be made in writing to the Data Protection Officer with proof of identity.

- **Right to data portability**

This means the right, at your request, to have your personal data transferred from us to another person or organisation, or to use your personal data from somewhere else. A request for portability must be made in writing to the Data Protection Officer with proof of identity.

- **Right to object**

This means the right to ask that your personal data is not used for profiling, direct marketing, profiling, automated decision-making (for example by a computerised process) and similar uses. An objection must be made in writing to the Data Protection Officer with proof of identity.

- **Rights related to automated decision making and profiling.**

This right enables you to object to the Council making significant decisions about you where the decision is completely automated and there is no human involvement. An objection must be made in writing to the Data Protection Officer with proof of identity

8 Data Retention

8.1 Personal Data which is no longer required will be destroyed appropriately. Personal Data will be destroyed in accordance with the Council's retention schedule.

9 Transfers to other Countries

9.1 Most of our processing occurs in the UK or European Union. This means that there are common standards for the processing of personal data.

10 Training

10.1 Data Protection training is important so that we can be sure that all employees and agency workers understand their responsibilities. All employees (including temporary employees) will complete Data Protection training every year and Elected Members will be offered the same training.

11 Information Commissioner Enforcement

11.1 The Information Commissioner has various enforcement powers at it's disposal ranging from inquiries into data breaches, Information Notices Assessment Notices, Enforcement Notices, Powers of Physical Entry and Inspection and, ultimately, Penalty Notices and Prosecution.

11.2 Penalty notices or monetary penalties (fines) may be served for non-compliance with the DPA and or serious data breaches. There are two levels as follows:

- The "higher maximum amount" is 20 million Euros (£17.6m)
- The "standard maximum amount" is 10 million Euros (£8.8m)

11.3 The maximum amount of penalty in sterling will be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

11.4 The "higher maximum" will apply to very serious and or damaging data breaches and fundamental failure to comply with the fundamentals of the DPA ideals.

11.5 All fines are made public by the Commissioner and the Chief Executive of the offending organisation is usually asked to make a formal undertaking to put in place effective measures and remedies.

11.6 If the organisation disputes the fine, it can appeal to the First-Tier Tribunal within 28 days of being informed of the Monetary Penalty Notice.

12 Contact, Information and Guidance

12.1 Requests for any information relating to rights or data protection matters should be made in writing to:

The Data Protection Officer
South Kesteven District Council
Council Offices
St Peters Hill
Grantham
Lincs
NG31 6PZ Email: dpo@southkesteven.gov.uk

12.2 Information can also be obtained from the Information Commissioner at:

The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
https://ico.org.uk

Telephone 0303 1231113 (local rate) or 0162 5545745 (national rate)

13 Non Compliance

13.1 Individual members of staff can face disciplinary action for misusing personal data. Malicious misuse and unauthorised disclosure of personal data can also lead to personal prosecution and/or liability to pay compensation in any civil action.

13.2 Elected Members when handling personal data in relation to Council business must comply with this policy. Malicious misuse and unauthorised disclosure of personal data can also lead to personal prosecution and/or liability to pay compensation in any civil action

14 Policy Review

14.1 This policy will be reviewed annually.

14.2 Reviews of this policy will take into account changes in the law, best practice, lessons learnt and changes in information technology (IT).

APPENDIX 1

PERSONAL DATA

Is identified by Article 4 of the GDPR as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic mental, economic, cultural or social identity of that natural person.”

SPECIAL CATEGORY DATA (SENSITIVE PERSONAL DATA)

Is identified by Article 9 of the GDPR as “data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of generic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.”

Special Category Data can only be processed by the Council if one or more specified statutory conditions apply. The statutory conditions are set out in summary below:

- Explicit consent (unless law prohibits the processing and that prohibition cannot be overridden by the person)
- Legal obligation on the controller in respect of employment, social security etc.
- Protection of the vital interests of the data subject or another person where the data subject is legally or physically incapable of giving consent
- Legitimate activities of a non-profit making organisation with a political, philosophical or trade-union aim
- The personal data is manifestly made public by the data subject
- Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Substantial public interest (based on a Union or State law which is proportionate to the aim pursued, respects the essence of the right to data

protection and provides specific measures to protect the fundamental rights and freedoms of the data subject)

- Necessary for the purposes of preventative or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care or treatment or the management of health and social care systems and services on the basis of Union or State law
- Public health (on the basis of Union or State law)
- Archiving in the public interest, research and statistics.

This page is intentionally left blank

South Kesteven District Council

Information Governance Guidance

May 2018

SOUTH KESTEVEN DISTRICT COUNCIL

Contents

1. Scope

1.1 This guidance applies to:

- All employees of the Council;
- Members of the Council;
- Suppliers and Contractors of the Council;
- Temporary and agency staff engaged by the Council;
- Volunteers at the Council;
- Others using the Council's information or systems.

1.2 The guidance covers all aspects of information within the Council, including (but not limited to):

- Personal and special category (sensitive) information (e.g. records about residents and staff);
- Other corporate information (e.g. financial or accounting records)

1.3 The guidance covers all information whether held in notes or structured records systems (paper and electronic) and the transmission of information (e.g. fax, e-mail, post and telephone etc.)

2. Purpose

2.1 'Information Governance' describes the framework by which organisations such as the Council handle information; it applies to special category (sensitive) and personal information of staff and also to information related to the business of the Council.

2.2 Effective Information Governance enables the Council to safeguard personal information and to make the best use of the information that it holds.

2.3 All staff have a responsibility at work to look after personal data properly and appropriately. Residents have a right to know that information about them is kept secure.

2.4 Breaches of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), through loss or mishandling of personal data, can result in large fines for the Council and disciplinary action against individual members of staff which may lead to dismissal.

2.5 Information is also a valuable asset that helps to ensure that the Council provides the best possible services to residents.

2.6 Information plays a key part in effective governance, service planning, financial management and performance management. It is therefore important that information is well-managed and used effectively to deliver and improve services.

2.7 The Council will actively protect all paper and electronic data and information in ways that are appropriate and cost effective. The Council will thereby fulfil its statutory responsibilities, protect the interests of residents, partners, suppliers and businesses, and maintain the quality, effectiveness and continuity of services to South Kesteven residents.

2.8 This guidance provides an overview of the Council's approach to Information Governance; a guide to the policies and procedures in use; and the roles and responsibilities for managing information to ensure compliance with legal requirements.

3. Protocol

3.1 The Council will implement information governance effectively to ensure the following:

3.1.1 **Keeping information safe and secure**

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained

3.1.2 **Recording accurately and only record what is required**

- Information will be supported by the highest quality data
- Only information that is required will be recorded

3.1.3 **Retaining and destroying records**

- Information will only be retained for as long as is required. Information will be destroyed securely as appropriate

3.1.4 **Accessible Information**

- Information will be accessible to those who have a right of access

3.2 The following ***information security principles*** guide this Protocol:

3.2.1 **Confidentiality** - Appropriate measures must be taken to ensure that information held by the Council is only accessible to those authorised to have access.

3.2.2 **Integrity** – The accuracy and completeness of information must be maintained and all changes or modifications affecting that information must be authorised, controlled and validated.

3.2.3 **Quality** - The Council must ensure that the information it holds is fit for its intended purpose.

3.2.4 **Availability** – Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Council's information and systems critical to the operation of key services and ongoing activities must be recoverable.

3.2.5 **Authentication** – Any person or system seeking access to Council information or networks must first establish their identity to the satisfaction of the Council.

3.2.6 **Access control** – Access to view or modify information or systems must be restricted to those whose job functions specifically require such access.

3.2.7 **Auditing** – User access and activity on each of the Council's computers, firewalls and networks must be recorded and maintained in compliance with security, retention and all legislative and regulatory requirements.

3.3 The Council will monitor this guidance document, and will update it as necessary.

4. Legislation and Standards

4.1 The following legislation and standards are an integral part of the regulatory environment within which the Council must operate:

- The GDPR;
- Data Protection Act 2018;
- Freedom of Information Act 2000
- Human Rights Act 1998
- Environmental Information Regulations 2004
- Local Government Act 1972
- Computer Misuse Act 1990
- Payment Card Industry Data Security Standard

5. Roles and responsibilities

5.1 The following roles and responsibilities underpin effective Information Governance within the Council.

5.2 Senior Information Risk Owner (SIRO)

This role provides senior leadership for information governance in the organisation. The role:

- Ensures effective governance arrangements are in place for improving the management of information in the Council;
- Oversees the development of policies, procedures and guidance;
- Identifies organisation-wide information management risks and ensures appropriate action to mitigate risks are agreed and implemented;
- Ensures effective training and staff development is in place;
- Oversees any communications needed about information governance;
- Provides an annual report and updates as required to Corporate Management Team about the delivery and success of the information governance action plan.

5.3 Assistant Directors / Directors

5.3.1 Are accountable for the implementation of Information Governance, policies, procedures and guidelines in their service area.

5.3.2 Take ownership of the information in their service area.

5.3.3 Are accountable for identifying and managing effectively the information necessary for service delivery.

5.4 Business Managers

5.4.1 Ensure that staff in their team(s) are aware of policies, procedures and guidance for Information Governance.

5.4.2 Ensure that the practice of managing information in their service area complies with policies, procedures and guidance.

5.4.3 Must report breaches in data protection to the Council's Data Protection Officer.

5.4.4 Identify risks in managing information in their service area and ensure these are mitigated and/or escalated as required

5.4.5 Ensure that members of staff attend relevant and appropriate training.

5.5 Data Protection Officer

5.5.1 To inform and advise the Council and its staff who carry out processing of their obligations pursuant to the GDPR.

5.5.2 To monitor compliance with the GDPR and the DPA and with the Data Protection Policy and other Data Protection Policies and Procedures.

5.5.3 To act as the contact point for the Information Commissioner's Office on all matters relating to data protection and to fully cooperate with this body.

5.6 All Staff (whether permanent or temporary) and others using Council systems or information

5.6.1 Have a responsibility to ensure that they are familiar with the contents of this Policy and to ensure information is managed in line with Information Governance policies, procedures and guidelines;

5.6.2 Must report breaches of data protection to their Manager;

5.6.3 Are to undertake training and support as required.

6. Training and Guidance

6.1 All Information Governance related guidance and procedures are published on the Council's intranet and available to all staff. Staff are made aware of these procedures through well-established management and communication channels – such as check ins and PDRs, team meetings, training, staff communication channels and communications campaigns. All employees are required to complete the mandatory e-learning module on GDPR.

7. Incident Management:

7.1 Clear guidance on incident management procedures should be documented and staff should be made aware of their existence, where to find them and how to implement them.

7.2 See Procedure for Reporting Information Security Breaches, Data Protection Breaches and Card Data Security Incidents www.southkesteven.gov.uk/CHttpHandler.ashx?id=24185&p=0 for further information.

This page is intentionally left blank

South Kesteven District Council

Procedure for reporting Information Security Breaches, Data Protection Breaches & Card Data Security Incidents

July 2018

SOUTH KESTEVEN DISTRICT COUNCIL

Introduction

This procedure applies to all staff and elected Members working for the South Kesteven District Council (The Council) and it applies to any actual, suspected or "near miss" loss of personal data.

Any loss of confidential information can result in large fines for the Council. The Council is under a duty to report certain types of breaches so it is imperative that these are reported as soon as possible.

This procedure should be used to report all breaches of confidentiality and information security whether actual or suspected. This covers information held and shared in different formats (paper, electronic or verbal).

This procedure underpins the Council's Information Governance guidance, www.southkesteven.gov.uk/CHttpHandler.ashx?id=24184&p=0 and our Data Protection Policy www.southkesteven.gov.uk/CHttpHandler.ashx?id=24182&p=0 which have been developed to protect the information handled by the Council. In addition, it supports the guidelines produced for connecting to the Government Secure Internet and is part of the Council's Payment Card Industry Governance.

All staff and Elected Members have a responsibility to report a suspected or actual breach of confidentiality or loss of data. Failure to do so may be considered a breach of the Council's Data Protection Policy and may result in disciplinary action.

Where there is a risk that Credit or Debit Card information may have been compromised, the Card Data Security Incident Response Plan, at Page 9 of this document, should also be followed.

Procedure

If you suspect an information security breach has occurred, you should report it immediately to the Council's Data Protection Officer (the DPO) as the Council is under a duty to report serious incidents within **72 hours** of becoming aware of them.

Breaches should be reported to dpo@southkesteven.gov.uk Telephone Number: 01476 406080

The DPO will conduct an initial investigation and risk assessment to ascertain the nature and seriousness of the incident. It is imperative that this assessment is done without delay.

If a breach meets the notification requirements, the DPO shall inform the Chief Executive of this fact. They will also inform the Information Commissioner as soon as possible and no later than 72 hours from the time the Council became aware of the breach. See Page 4 for guidance on this.

The DPO does not need to have full details of the breach available prior to making a notification to the Information Commissioners Officer (ICO). If the DPO believes, on initial assessment, that there is a likelihood that the breach will meet the notification requirements then the DPO should make the initial notification within 72 hours and update the ICO as and when further information becomes available.

The DPO will maintain a record of incidents, including a risk assessment, the outcomes and resulting recommendations made.

Breach Management Team

The Council's DPO will, if they consider it necessary, chair a breach management team to assist in responding to a breach. The exact makeup of this team will depend on the nature and the seriousness of the breach and what skills and resources are required to respond.

The core team should comprise representatives from IT Services, Legal Services, Risk & Audit, Human Resources and Communications as well as representatives from the effected service area(s). The makeup of the team will depend on the exact nature of the breach.

Guidance

What is a personal data breach?

Breaches can be categorised according to the following three well-known information security principles:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data.

- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

- **Integrity breach** - where there is an unauthorised or accidental alteration of personal data.

A breach may involve a combination of these elements.

Assessing Risk and High Risk

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the ICO is only triggered where a breach is likely to result in a 'risk to the rights and freedoms of individuals'.
- Communication of a breach to the individual is only triggered where it is likely to result in a 'high risk to their rights and freedoms'.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. This includes loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include other significant economic or social disadvantage to those individuals.

A breach will be considered to pose a high risk to the rights and freedoms of individuals where the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation.

When the breach involves sensitive, or special category, personal data that reveals racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, or trade union membership, or includes genetic data and biometric data for the purpose of identifying a natural person, data concerning health or data concerning sex life or sexual orientation, or criminal convictions and offences or related security measures, it should be assumed that there will be a high risk to the rights and freedoms of individuals.

Factors to take into account

- Nature of the breach
- Nature, sensitivity and volume of the data
- Ease of identification
- Severity of consequences for data subject(s) - for instance identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm
- If there has been a loss of confidentiality is the 3rd party "trusted"? - The fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the ICO, or to the affected individuals.
- Special characteristics of the individual (children, vulnerable adults etc.)
- The number of affected individuals

Notification of a personal data breach

1. Notifying the ICO

The GDPR and Data Protection Act 2018 makes it mandatory for serious data breaches to be reported to the ICO.

Where a breach is likely to result in a risk to the rights and freedoms of natural persons, a notification to the ICO should be made within **72 hours** of the Council (not the DPO) becoming aware of the breach.

Where a notification to the ICO is not made within 72 hours, it shall be accompanied by written reasons for the delay.

The notification needs to:

(a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) Communicate the name and contact details of the DPO or other contact point where more information can be obtained;

(c) Describe the likely consequences of the personal data breach;

(d) Describe the measures taken or proposed to be taken by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible to provide all the above information at the same time, it may be provided in phases without undue further delay.

The Council is required to record the following information in relation to a personal data breach:

(a) The facts relating to the breach,

(b) Its effects,

(c) The remedial action taken.

It must be recorded in such a way as to enable the ICO to verify compliance.

2. Notifying data subjects affected by the breach

The Council is also required to communicate a breach to the affected individuals where the breach is likely to result in a high risk to the rights and freedoms of natural persons.

This a higher risk level than notification to the ICO.

Where a breach poses a high risk, the Council should communicate the personal data breach to the data subject without undue delay.

The communication shall describe in clear and plain language:

(a) A description of the nature of the breach;

(b) The name and contact details of the DPO or other contact point where more information can be obtained;

(c) The likely consequences of the personal data breach;

(d) The measures taken, or proposed to be taken, by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Circumstances where notification of the data subject is not required:

(a) When the data is protected, measures that render personal data unintelligible or inaccessible to any person who is not authorised to access it.

(b) Immediately following a breach, the Council has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.

(c) It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. Instead, the Council must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.

The Council may restrict, wholly or partly, the provision of information to the data subject by way of notification to:

(a) Avoid obstructing an official or legal inquiry, investigation or procedure;

(b) Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

(c) Protect public security;

(d) Protect national security;

(e) Protect the rights and freedoms of others.

Appendix 1 – Breach Reporting Form			
Reporting Officer			
Team			
Service Area and name of Business Manager			
Date of Breach			
Date Breach discovered			
Date Reported to the ICO			
Please provide a brief explanation for any delay between the breach being discovered and the ICO being notified			
Does the breach involve sensitive / special category personal data?	YES	NO	Unknown at time of reporting
Does the breach involve card data?	YES	NO	Unknown at time of reporting
A description of the breach – what caused it, what data was affected, what was / could be the impact of the breach?			

To be completed by the Data Protection Officer			
Risk Assessment?	**HIGH**	**MEDIUM**	**LOW**
Reported to the ICO?	**YES**		**NO**
Date reported to the ICO			
If ICO not notified, record the reason why			
Data subjects informed?	**YES**		**NO**
Date data subjects informed			
If data subjects not informed, record the reason why			
Describe the steps taken to remedy the breach / recover the data or to mitigate the risk and impact of the breach			

Post breach analysis, follow up actions and lessons learnt	

A copy of this form will be retained by the Data Protection Officer.

Card Data Security Incident Response Plan

Scope

This plan applies to all staff and contractors working for the Council.

Purpose

To address cardholder data security, the major card brands (Visa, MasterCard, etc.) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants document an incident response plan.

Any compromise of cardholder data can result in large fines for the Council and reputational damage. All staff have a responsibility to protect cardholder data.

This procedure should be used to report all incidents, whether actual or suspected. This covers information held and shared in different formats (paper, electronic or verbal).

The procedure underpins the Council's Information Governance Policy and Data Protection Policy, which have been developed to protect the information handled by South Kesteven District Council.

A data compromise, or breach, occurs when a person accesses the Council's customer's information with the intent to commit fraud. The information most valuable to criminals include the customer's card number, expiry date, name, address and the security details such as CVC / CVV code and the track data. A cardholder data compromise is any situation where theft or suspected theft of cardholder data has occurred.

Criminals may access cardholder data in a number of ways including:

- Theft from premises of terminals and terminal receipts,
- A dishonest member of staff accessing and passing on cardholder data to criminals,
- A criminal tampering with a card terminal and skimming data,
- Through the Council's third party payment providers.

Procedure

If you suspect an information security breach has occurred, you should report it immediately to your line manager and / or your Business Manager.

If a card terminal has (or is suspected to have been) tampered with, unplug the device and Contact the IT service desk. They will collect the terminal. IT Services can provide spare CAPITA terminals and the Control Accounting Team can arrange for a replacement Global Pay terminal (contact details below).

Business Managers must report the incident to:

- The Council's SIRO (Senior Information Risk Officer)
- The Control Accounting Team

The Control Accounting Team will immediately inform the Relationship Manager for the Council's Merchant Services Provider and ensure the payment brands are advised within the necessary timescales. If a card terminal has been stolen or compromised, the Control Accounting team will follow the UK Cards Association procedures.

The Control Accounting Team will inform the Council's:

- Data Protection Officer, dpo@southkesteven.gov.uk, who will liaise with the IT team, and instigate any necessary remedial action.

The Council's Data Protection Officer will maintain a record of incidents, the outcomes and any recommendations made.

In Addition

To minimise further data loss, and preserve evidence to facilitate the investigation process, the Council will not:

- Access, alter or delete files in the compromised system(s)
- Attempt to change passwords on the compromised system(s).
- Log in as administrators - indeed logon at all.
- Turn (back) on the compromised system(s).

Any logs generated are kept for at least six months in keeping with HMG GPG13.

While no system is 100% secure, South Kesteven District Council:

- Carry out active scans for credit and debit card data on any data stored and transmitted via email, and prevent this from onwards transmission.
- Have controls on USB's being added to computers, which makes the movement of skimming of data more difficult from Council computer systems.
- Only employ 3rd party payment providers who are PCIDSS compliant and listed on the Visa Europe Member or Merchant Agent Web listing.
- Ensure staff are trained in awareness in relation to card terminal tampering.

- Have specific technical controls in place within the Contact Centre as well as governance and training in relation to processing card payments.

Procedure for undertaking a Data Protection Impact Assessment

July 2019

SOUTH KESTEVEN DISTRICT COUNCIL

1. Introduction

1.1 Under previous legislation, the carrying out of a Data Privacy Impact Assessment (DPIA) was good practice. Completing a DPIA is now mandatory in certain circumstance in both the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). If you are introducing, changing or assessing a process that handles personal data, you must complete a DPIA. This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance.

1.2 A DPIA is a process to help identify and minimise the data protection risks of a particular project or activity when the processing of personal data is likely to result in 'high risk to individuals' rights or freedoms'. A high risk might arise if the Council is intending to process data that:

- Involves the use of special category (sensitive), or highly personal data;
- Concerns vulnerable adults or children;
- Involves preventing people from using a service or exercising a right;
- Includes processing data on a large scale.

1.3 If you are in any doubt as to whether you need to complete a DPIA, you should consult with South Kesteven District Council's Data Protection Officer. Email: dpo@southkesteven.gov.uk

1.4 If you identify a high risk and you cannot mitigate that risk, you must consult with the DPO who will contact the Information Commissioner's Office (ICO) before starting the processing. The ICO will give written advice within 8 weeks, or 14 weeks in complex cases. In appropriate cases, the ICO has the power to issue a formal warning not to process the data, or to ban the processing altogether.

2. When should a DPIA be undertaken?

2.1 A DPIA is a process to systematically analyse the Council's processing and help SKDC to minimise data protection risks. It is intended to be an ongoing process; it should be monitored and reviewed as necessary. A DPIA must:

- Describe the processing and its purposes;
- Assess necessity and proportionality;
- Identify and assess risks to individuals; and
- Identify any measures to mitigate those risks and protect the data.

2.2 The GDPR states that the Council must carry out a DPIA if it plans to:

- Systematically monitor a public place on a large scale by for example, installing CCTV cameras;
- Process sensitive personal data or criminal offence data on a large scale;
- Use systematic and extensive profiling with significant effects;
- Use new technologies, process biometric data (e.g. fingerprints, facial recognition, retinal scans) and geometric data (an individual's gene sequence);
- Profile children or target services at them;
- Match data or combine data sets from different sources;
- Process personal data without providing a privacy notice directly to an individual;
- Process personal data that might endanger an individual's health or safety in the event of a security breach.

2.3 The GDPR also provides that the Council must, where appropriate, seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

The following checklist will assist you in terms of determining whether a DPIA must be carried out.

		DPIA questions	**Yes/No**
1.	**Identity**	Will the project involve collecting information about individuals for the first time?	
2.	**Identity**	Will your project or activity compel individuals to provide information about themselves?	
3.	**Sharing information**	Will any information about individuals be disclosed to any other organisations?	
4.	**Data**	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
5.	**Data**	Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition or CCTV cameras?	

6.	**Data**	Will the project result in you making decisions or taking action against individuals in ways that could have a significant impact on them?	
7.	**Data**	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	
8.	**Data**	Will the project or activity require you to contact individuals in ways that they may find intrusive?	

If you have answered YES to ANY of the questions in the checklist, you will need to consult with the DPO.

3. What should a DPIA contain?

3.1 Section 64 of the DPA 2018 prescribes that a DPIA must contain as a minimum:

- A systematic description of the proposed processing and its purpose;
- An assessment of the risks to the rights and freedoms of data subjects;
- The measures proposed to address those risks;
- Safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Council's revised Data Protection Policies and Procedures.

The following Data Protection Impact Assessment Template should be used when carrying out a DPIA.

Team / Service:	
Information Asset Owner:	
Team / Service Contact:	
Brief description of processing being assessed:	
Director / project sponsor:	

Version	Date	Author	Change

Section A – Description of processing and consultation

A.1 Tell us what you are trying to do and why?
Title of Project/process: What is the Project/process? What is the purpose of the project/process? How will you be processing personal data?

A.2 Describe who has been consulted while designing/reviewing this process.

A.3 What personal and/or sensitive personal data will be collected?
Detail the risks involved when processing the data for this purpose. What Personal Data will be collected (list all fields): What sensitive personal data will be collected (list all):

A.4 Risk assessment.
Detail the risks involved when processing the data for this purpose.

Section B – Data Protection Principles

This section asks you to indicate how the processing complies with each data protection principle. Where you can, please provide evidence of what you have in place to achieve compliance, or clearly state what work is underway where you know there are gaps. You can provide links to existing documents, or send attachments with your DPIA.

Principle 1: Lawfulness, Fairness and Transparency

- When we process personal we must make sure that we have a lawful reason for doing so, our use of the data is fair, and we tell people what we are doing and why.
- We must identify a lawful reason to process the personal data. This is known as a 'Condition of Processing'.

B.1.1 What is the legal basis for processing the data? (delete the conditions that do not apply)
The legal basis for processing information is set out in the General Data Protection Regulation (GDPR), articles: • 6.1(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; • 6.1 (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; • 6.1 (c) processing is necessary for compliance with a legal obligation to which the controller is subject; • 6.1 (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; • 6.1 (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; • 6.1 (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

- When we collect personal data, we must be clear about why we need it and what we will do with it. This information should be clearly explained in privacy notices.

B.1.3 What information is being provided to data subjects to ensure that they are aware of this processing?
Provide information on how data subjects will be (or are) made aware of this processing:

Principle 2: Purpose limitation

- Where we have collected personal data for a particular purpose, we cannot use it for another purpose simply because we hold it. The only exception to this is if we are required to process data by law.
- It is important the DPIA reflects all the purposes for which personal data is used so it is not processed in a way that data subjects would not expect. This also ensures that privacy information can be assessed to be comprehensive and complete.

B.2.1 If you are using existing data for a new purpose, or the data you are collecting may be used in a different way to the processing primarily described in A.1, explain the alternative processes here.

Principle 3: Data Minimisation

- When designing processes that handle personal data, it is important that we only collect, use, and/or share personal data which is relevant and necessary. We should clearly identify what personal data is necessary for a process and why.

B.3.1 List the types of personal data which will be collected and/or processed? Indicate why it is necessary/relevant.
Personal data is information that relates to an identified or identifiable individual. This could be a name or a number or could include other identifiers such as an IP address or a cookie identifier, or other factor. Consider if the individual is still identifiable. You should look at the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual.

B.3.2 What special category data will be processed?
Special category data is defined in the GDPR as: • *race* • *ethnic origin* • *politics* • *religion* • *trade union membership* • *genetics* • *biometrics (where used for ID purposes)* • *health* • *sex life* • *sexual orientation*

B.3.4 Describe how the personal data will be collected.
Describe how data is collected and where it is stored for the process.

Principle 4: Accuracy

- Personal data must be accurate and, where necessary, kept up to date. Reasonable steps should be taken to routinely review personal data which is likely to change over time, and procedures should be in place to rectify any personal data that is found to be inaccurate.

B.4.1 Describe how the accuracy of personal data will be monitored and maintained.

Principle 5: Storage Limitation

- All records held by the Council should be retained in accordance with the Record Retention Schedule.
- Our systems and processes should be designed to delete personal data as soon as it is no longer needed. This might mean that parts of records can be deleted at different times.

B.5.1 Indicate the retention rule (including reference) from the Record Retention Schedule which will be applied to this processing.

Principle 6: Security, Integrity and Confidentiality

- Personal data should be protected against unauthorised access, accidental loss, destruction or damage. There should be appropriate governance controls in place (including physical and technical controls) to ensure that personal data is secure and only accessed by those who are authorised to do so.
- When introducing new systems or software which will store or transmit personal data, it is important that we understand what security is in place to protect the information. It will often be necessary for this type of information to be sought from the system supplier.

B.6.1 What risks are have been identified which may lead to data being processed in a way which is not intended?

B.6.2 Describe who will have access to the data?

B.6.3 Describe what organisational controls will be in place to support the process and protect the data.

B.6.4 Describe what technical controls will be in place to support the process and protect the data.

B.6.5 Will the data be routinely shared with any other service or organisation? If yes, indicate whether there is an information sharing agreement, or relevant contract clauses, in place to govern how personal data is treated.

B.6.6 Will data be stored outside the European Economic Area (EEA)? If yes, include evidence of contract clauses which ensure that personal data is maintained in accordance with UK data protection legislation.

B.6.7 Given the controls in place, what is the likelihood and severity of threats identified in B.6.1 taking place?
Impact: **Likelihood**:

Section C – Individual Rights

- Data protection legislation provides data subjects with certain rights about their data. The DPO has a responsibility to co-ordinate all requests from data subjects who wish to exercise their rights but it is important that processes are designed to support these.

Please indicate whether the following controls are in place. Refer to the checklist to understand when some rights might not be applicable to the processing described.

Right/Control	Yes	No	N/A
Right to be informed – privacy information is in place (or planned) to tell people what we will do with their data (B.1.3)			
Right to access personal data – procedures are in place to ensure that requests to access personal data are dealt with according to Council policy			
Right to rectification – processes are in place which allow inaccurate personal data to be rectified (B.4.1)			
Right to erasure – record retention rules are consistently applied to all data (B.5.1).			
Right to restrict processing - procedures are in place to ensure that requests to restrict processing are dealt with according to Council policy			
Right to data portability - procedures are in place to ensure that requests to transfer data are dealt with according to Council policy			
Right to object to processing - procedures are in place to ensure that objections to processing are dealt with according to Council policy			

Section D – Risk Management

D.1.1 What controls are in place to manage or mitigate any risks and have you considered whether there is a need to consult with data subjects?

Section E – Submission

Once completed, send this form, and any accompanying evidence to: DPO@southkesteven.gov.uk

The DPIA will be reviewed by Data Protection. The risk will be assessed, and you will receive a response that outlines:

- current compliance with the data protection principles based upon what has been described within the DPIA
- identify and assess outstanding risks associated with the proposed processing and, if necessary, recommended improvement actions.
- Recommended actions must be addressed prior to the commencement of the processing.

When this has been completed the DPIA will be sent to the Director/project sponsor to review and accept responsibility for the identified risks and mitigation of those risks.

South Kesteven District Council

Protocol for protecting personal information

June 2018

The Council has a duty to protect the information held about members of the public.

Breaches of the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) can result in enforcement action being taken against the Council by the Information Commissioner's Office (ICO), and a fine of up to 20 million Euros being imposed. This in turn can lead to disciplinary action being taken against individual members of staff responsible for the data breach.

For protecting personal and special category (sensitive) data:

1. **Always keep personal information safe and secure**
2. **Check who you are sharing information with**
3. **Use email carefully and responsibly**
4. **Do not store personal data on laptops and mobile devices**
5. **Keep data secure when working away from the office**
6. **Take extra care when taking information out of the office**
7. **Always report information security breaches**

1. Always keep personal information safe and secure

- Always ensure that records containing personal and special category (sensitive) data are stored securely to prevent unauthorised access. If you have paper records you must store these in a locked cabinet or drawer. You can see the definition of personal and special category (sensitive) data in the Council's Data Protection Policy www.southkesteven.gov.uk/CHttpHandler.ashx?id=24182&p=0

- Do not use the hard drive (the C: drive) on your desktop computer or laptop for saving and storing personal data. This is not secure and back-up copies of records are not made by IT networks.

- Never share any of your IT system passwords with anyone else.
  Passwords should not be written down. Passwords should be a minimum of 8 characters in length, and use a mix of letters, numbers and other characters. Do not use the same password for different systems.

- Ensure that your desk and computer cannot be overlooked by members of the public. Where you are processing special category (sensitive) personal information you should also consider whether care should be taken to prevent other members of staff from seeing the work.

- Be security aware when entering or leaving the office. Do not let unauthorised persons into the building. If someone asks to be let into the office or tries to follow you through the secure doors, politely ask to see their ID.

- When records no longer need to be kept (in line with the Council's Retention Schedule. All personal information held in hard copy should be disposed of appropriately using the confidential waste bins provided.

- When using the printer, photocopier or scanner please check that all documents are collected when you have finished. Check that the documents you pick up are the correct ones.

- Before sending a letter always check that the address is correct and that it is addressed to the correct recipient. Double-check any documents that are being enclosed to make sure they are the correct ones.

- You should avoid sending sensitive records by fax unless there is no other secure alternative. Before sending a fax check with the recipient that the fax number is correct and make the recipient aware that the fax is being sent. Always take care to ensure that the correct number is inputted into the fax machine. You may wish to ask a colleague to assist you.

- You must only use authorised Council USB memory sticks. The use of any other device with Council equipment risks damaging systems. Contact your Business Support team or the IT Service Desk for assistance with this.

2. Check who you are sharing information with

- If you are sharing personal and/or special category (sensitive) data, you must make sure that the person you are sharing the data with has a need and right to have access to the data. The disclosure of data must be authorised by the owner of that information (asset) and lawful.

- Be careful about sharing information via the telephone. Take simple steps to verify the caller's identity to establish their identity.

- Requests for disclosure by law enforcement agencies should be made in writing.

- Members of staff must only access personal information and systems where it is necessary for their role. **Remember** - it is a disciplinary offence to use or access the Council's records for your own purposes.

- Do not discuss or share Council-owned personal data via social media. Only authorised members of staff should use social media for Council purposes.

3. **Use email carefully and responsibly**

   - All email for Council business must be sent using the Council's email systems. Personal email accounts must not be used for council business.

   - When sending an email, care must always be taken to ensure that it has been addressed to the appropriate person and that the correct email address has been used.

   - When sending bulk email it is important to use the 'blind carbon copy' function (Bcc) to prevent the inadvertent disclosure of email addresses.

   - When sending emails involving special category (sensitive) content, use simple anonymisation techniques to mitigate the risks of unauthorised or accidental disclosure. For instance, use reference numbers and initials rather than names. The intended recipient will know who the information relates to but an unintended recipient will not be able to identify the subject of the email.

   - Be aware of the risks posed by spam email containing viruses and malware. Whilst the Council has good anti-virus software in place, members of staff should be alert to any email that seems odd or unusual, for instance it looks out of place, is poorly spelt, contains an offer that is too good to be true etc. If you receive a suspect email do not click on any link or open an attachment it may contain but report it to IT immediately.

4. **Do not store personal data on laptops or mobile devices**

   - Personal data should only be stored on the Council's secure network.

   - Due care and attention should be used when working on laptops or other devices when away from your normal place of work. Make sure you cannot be overlooked and never leave your equipment unattended or lend it to a third party.

   - Only use Council issued or Council approved laptops or mobile devices. Elected Members are permitted to use one piece of their own IT equipment. This is purely for the purposes of accessing Council e-mail and must be used in accordance with the Acceptable Use of IT Policy http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=22433&p=0

5. **Keep data secure when working away from the office**

   - Files, paperwork and mobile computing devices must be stored in a secure location when not in use. Store any manual records separately from your IT equipment.

- Council data should not be stored at home long term. If you are to be out of the office for a significant period of time, you should ensure that all Council owned personal data is returned to the office.

- If you are leaving the Council's employment you must return all Council owned data and equipment to the Council in good time.

- A record of any files or records taken out of the office should be kept in case they are damaged/destroyed, lost or stolen. Where possible you should avoid taking original files or records out of the office.

- The Council recognises that there are circumstances when personal information will need to be taken out of the office.

- Only transport the minimum of personal information required. Ensure that you don't leave files, equipment or bags containing Council equipment or Council personal data unattended at any time or on view in a locked vehicle.

- When travelling on public transport, extra care should be taken to ensure that bags containing personal information are not lost or stolen.

- You must ensure that any electronic media has been appropriately encrypted. Only Council owned electronic transportable media should be used.

- The password (encryption key), which provides access to information being sent by any electronic media or email, must be sent to the recipient by a different method to that by which the data has been sent.

- It is good practice to keep a record of any large-scale data transfers. The record should show what data was sent, how it was sent, and what security measures were taken. All large-scale transfers of personal data must be authorised by the Assistant Director of the information asset owner's area. If in doubt, seek legal advice from the Council's Data Protection Officer.

- Where possible you should avoid working on or discussing work involving personal or sensitive matters in a public environment. If this is not possible, care should always be taken to ensure that you are not overlooked or overheard.

6. Always report information security breaches

- All staff have a responsibility to report a suspected or actual breach of confidentiality or loss of data. Early notification of an incident can ensure that any mitigating or recovery actions can take place as soon as possible. It is better to report a suspected incident even if you are unsure if one has occurred, than not to do so.

- If you suspect an information security breach has occurred, you should report it immediately to your line manager and your Business Manager.

- Business Managers must report the incident to the Councils Data Protection Officer.

- Breaches will be dealt with in line with the Council's Procedure for Reporting Information Security Breaches, Data Protection Breaches and Card Security Incidents
  www.southkesteven.gov.uk/CHttpHandler.ashx?id=24185&p=0

- There is a statutory duty on the Council to notify the Information Commissioner's Office of the above within **72 hours**. Failure to do so can result in a fine of up to 10 million Euros being imposed on the Council.

Appendix 1 – Breach Reporting Form			
Reporting Officer			
Team			
Service Area and name of Business Manager			
Date of Breach			
Date Breach discovered			
Does the breach involve the personal data of living individual(s)?	YES	NO	Unknown at time of reporting
Does the breach involve special category personal data?	YES	NO	Unknown at time of reporting
Does the breach involve card data?	YES	NO	Unknown at time of reporting
A description of the breach: **1/ what caused it?** **2/ what data was affected?** **3/ what was / could be the impact of the breach?**			
Do you consider the data to be contained and the risk to data subjects mitigated?	YES – Explain NO – Explain		

To be completed by the Data Protection Officer			
Risk Assessment?	**HIGH**	**MEDIUM**	**LOW**
Reported to the ICO?	**YES**		**NO**
Date reported to the ICO			
If ICO not notified, record the reason why			
Data subjects informed?	**YES**		**NO**
Date data subjects informed			
If data subjects not informed, record the reason why			
Describe the steps taken to remedy the breach / recover the data or to mitigate the risk and impact of the breach			
Post breach analysis, follow up actions and lessons learnt			

South Kesteven District Council

Data Protection Policy

December 2020

CONTENTS

1 Introduction

1.1 This is South Kesteven District Council's Data Protection Policy.

1.2 South Kesteven District Council processes personal data to carry out its duties and obligations. This policy sets out the Council's commitment to protecting and handling personal data.

2 Scope

2.1 This Policy applies to:

- All employees of the Council;
- Members of the Council;
- Suppliers and Contractors of the Council;
- Temporary staff engaged by the Council;
- Volunteers at the Council;
- Others using the Council's information or systems

2.2 Some of the Council's obligations in this policy are supported by other policies and procedures, where relevant, links to those policies and procedures are provided in this document.

2.3 This policy relates to personal data, which means any information in paper or digital format relating to a person who can be identified by that information. Personal data may also be classed as special category data. The definitions of personal and special category data are attached at Appendix 1.

3 Data Protection Principles

3.1 South Kesteven District Council must protect and process the personal data, which it holds in accordance with data protection principles established by law. The Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR), require us to be sure that all personal data is:

- Processed fairly, lawfully and in a transparent manner ('lawfulness, fairness and transparency');
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation');
- Adequate, relevant and limited only to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- Accurate and where necessary kept up to date, erased or rectified without delay ('accuracy');
- Kept in a form which permits identification of data subjects for no longer than is necessary ('storage limitation');
- Processed in accordance with the rights of data subjects
- Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4 General requirements

4.1 The main requirements for data protection are that:

- Personal data will only be accessed by those who need it for work purposes
- Personal data will not be divulged or discussed except when performing normal work duties
- Personal data must be kept safe and secure at all times, including at the office, public areas or in transit

- Personal data will be regularly reviewed and updated
- Internal and external queries about data protection to the Council must be dealt with effectively and promptly

4.2 How the Council complies with these requirements is set out in:
IT Security Policy http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=24180&p=0
Acceptable Use of IT Policy
http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=24181&p=0
Protocol relating to the protection of personal data
www.southkesteven.gov.uk/CHttpHandler.ashx?id=24183&p=0

5 Information Sharing

5.1 Personal data may need to be shared with other organisations in order to deliver our services or perform our duties. This can only be done where we have permission or if there is a legal obligation for us to share personal data.

5.2 Where the Council regularly shares personal information with our partners and other organisations an Information Sharing Agreement will be put in place. This agreement is signed by all partners to the sharing and agrees a set of standards and best practice surrounding Data Protection. However, these are not needed when information is shared in one-off circumstances but a record of the decision and reasons for sharing information will be kept.

5.3 All Data Sharing Agreements will be registered with the Council's Data Protection Officer. That officer will maintain a register of all our Data Sharing Agreements.

5.4 Where we give personal data or give access to personal data that we hold to anybody acting on behalf of the Council, we will require that party to sign a Non-Disclosure Agreement.

6 Data Privacy Impact Assessments (DPIAs)

6.1 DPIAs will be completed to help identify and minimise risks to the protection of data in the following situations where personal data is held by the Council:

- At the beginning of a new project or when implementing a new system
- Before entering a data sharing agreement
- When major changes are introduced into a system or process

For further guidance on undertaking Data Protection Impact Assessments (DPIA's), please read:
Procedure for Undertaking a Data Protection Impact Assessment
www.southkesteven.gov.uk/CHttpHandler.ashx?id=24187&p=0

7 Data Subject Rights

7.1 The Council is committed to ensuring individuals can freely exercise their rights. Below is a summary of those rights.

Right to Access - This allows the individual to ask the Council if it holds personal information about them, what it uses the information for and to be given a copy of that information**.** Anyone wanting to know what personal data the Council holds about them can make a Subject Access Request by completing "Subject Access Information Request Form". This form and the procedure for making applications and dealing with SAR's is available on this link: http://www.southkesteven.gov.uk/index.aspx?articleid=8460

Right to correct incorrect information (rectification) - This means the right to have your personal data corrected if the data we hold is not correct, or completed if it is incomplete. A request for a correction must be made in writing to the Data Protection Officer with proof of identity.

Right to erasure - This means you have a 'right to be forgotten' and all your personal data deleted in certain circumstances. A request for erasure must be made in writing to the Data Protection Officer with proof of identity.

Right to restriction of processing of personal data in certain circumstances - This means that you can ask us to limit the way that we use your personal data in some situations. A request for restriction must be made in writing to the Data Protection Officer with proof of identity.

Right to data portability - This means the right, at your request, to have your personal data transferred from us to another person or organisation, or to use your personal data from somewhere else. A request for portability must be made in writing to the Data Protection Officer with proof of identity.

Right to object - This means the right to ask that your personal data is not used for profiling, direct marketing, profiling, automated decision-making (for example by a computerised process) and similar uses. An objection must be made in writing to the Data Protection Officer with proof of identity.

Rights related to automated decision making and profiling - This right enables you to object to the Council making significant decisions about you where the decision is completely automated and there is no human involvement. An objection must be made in writing to the Data Protection Officer with proof of identity.

8 Data Retention

8.1 Personal Data which is no longer required will be destroyed appropriately. Personal Data will be destroyed in accordance with the Council's retention schedule.

9 Transfers to other Countries

9.1 Most of our processing occurs in the UK or European Union. This means that there are common standards for the processing of personal data.

10 Training

10.1 Staff training ensures the organisation is compliant with legislative requirements and provides employees with the knowledge of their responsibility to keep personal data secure.

10.2 All employees must complete Data Protection training annually (including temporary employees). Members will complete data protection awareness sessions at Member induction. They will also be offered Data Protection training within the Members Development programme.

11 Information Commissioner Enforcement

11.1 The Information Commissioner has various enforcement powers at its disposal ranging from inquiries into data breaches, Information Notices Assessment Notices, Enforcement Notices, Powers of Physical Entry and Inspection and, ultimately, Penalty Notices and Prosecution.

11.2 Penalty notices or monetary penalties (fines) may be served for noncompliance with the DPA and serious data breaches. There are two levels as follows:

- The "higher maximum amount" is 20 million Euros, or 4% of the organisation's annual revenue from the preceding financial year, whichever amount is higher.
- The "standard maximum amount" is 10 million Euros, or 2% of the organisation's annual revenue from the preceding financial year, whichever amount is higher.

11.3 The maximum amount of penalty in sterling will be determined by applying the spot rate of exchange set by the Bank of England on the day on which the penalty notice is given.

11.4 The “higher maximum” will apply to very serious and or damaging data breaches that fail to comply with the fundamentals of the DPA principles.

11.5 All fines are made public by the Commissioner and the Chief Executive of the offending organisation is usually asked to make a formal undertaking to put in place effective measures and remedies.

11.6 If the organisation disputes the fine, it can appeal to the First-Tier Tribunal within 28 days of being informed of the Monetary Penalty Notice.

12 Contact, Information and Guidance

12.1 Requests for any information relating to rights or data protection matters should be made in writing to:

The Data Protection Officer
South Kesteven District Council
Council Offices
St Peters Hill
Grantham
Lincs
NG31 6PZ
Email: dpo@southkesteven.gov.uk

12.2 Information can also be obtained from the Information Commissioner at:

The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9
5AF
https://ico.org.uk
Telephone 0303 1231113 (local rate) or 0162 5545745 (national rate)

13 Non-Compliance

13.1 Individual members of staff can face disciplinary action for misusing personal data. Malicious misuse and unauthorised disclosure of personal data can also lead to personal prosecution and/or liability to pay compensation in any civil action.

13.2 Elected Members when handling personal data in relation to Council business must comply with this policy. Malicious misuse and unauthorised disclosure of personal data can also lead to personal prosecution and/or liability to pay compensation in any civil action.

14 Policy Review

14.1 This policy will be reviewed every two years or where significant changes to legislation occur.

14.2 Reviews of this policy will take into account changes in the law, best practice, lessons learnt and changes in information technology (IT).

APPENDIX 1

PERSONAL DATA

Is identified by Article 4 of the GDPR as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic mental, economic, cultural or social identity of that natural person."

SPECIAL CATEGORY DATA (SENSITIVE PERSONAL DATA)

Is identified by Article 9 of the GDPR as "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of generic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Special Category Data can only be processed by the Council if one or more specified statutory conditions apply. The statutory conditions are set out in summary below:

- Explicit consent (unless law prohibits the processing and that prohibition cannot be overridden by the person)
- Legal obligation on the controller in respect of employment, social security etc.
- Protection of the vital interests of the data subject or another person where the data subject is legally or physically incapable of giving consent
- Legitimate activities of a non-profit making organisation with a political, philosophical or trade-union aim
- The personal data is manifestly made public by the data subject
- Necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- Substantial public interest (based on a Union or State law which is proportionate to the aim pursued, respects the essence of the right to data protection and provides specific measures to protect the fundamental rights and freedoms of the data subject)
- Necessary for the purposes of preventative or occupational medicine, assessment of working capacity, medical diagnosis, provision of health or social care or treatment or the management of health and social care systems and services on the basis of Union or State law
- Public health (on the basis of Union or State law)
- Archiving in the public interest, research and statistics.

This page is intentionally left blank

South Kesteven District Council

Information Governance Guidance

December 2020

CONTENTS

1 Scope

1.1 This guidance applies to:

- All employees of the Council;
- Members of the Council;
- Suppliers and Contractors of the Council;
- Temporary and agency staff engaged by the Council;
- Volunteers at the Council;
- Others using the Council's information or systems.

1.2 The guidance covers all aspects of information within the Council, including (but not limited to):

- Personal and special category data (e.g. records about residents and staff);
- Other corporate information (e.g. financial or accounting records)

1.3 The guidance covers all information whether held in notes or structured records systems (paper and electronic) and the transmission of information (e.g. email, post and telephone etc.)

2 Purpose

2.1 'Information Governance' describes the framework by which organisations such as the Council handle information; it applies to special category (sensitive) and personal information of staff and also to information related to the business of the Council.

2.2 Effective Information Governance enables the Council to safeguard personal information and to make the best use of the information that it holds. Acknowledging the ways, a council acting commercially may use and share data whist ensuring compliance with current data protection laws.

2.3 All staff have a responsibility at work to look after personal data properly and appropriately. Residents have a right to know that information about them is kept secure.

2.4 Breaches of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), through loss or mishandling of personal data, can result in large fines for the Council and disciplinary action against individual members of staff which may lead to dismissal, where actions were intentional.

2.5 Information is also a valuable asset that helps to ensure that the Council provides the best possible services to residents.

2.6 Information plays a key part in effective governance, service planning, financial management and performance management. It is therefore important that information is well-managed and used effectively to deliver and improve services.

2.7 The Council will actively protect all paper and electronic data and information in ways that are appropriate and cost effective. The Council will thereby fulfil its statutory responsibilities, protect the interests of residents, partners, suppliers and businesses, and maintain the quality, effectiveness and continuity of services to South Kesteven residents.

2.8 This guidance provides an overview of the Council's approach to Information Governance; a guide to the policies and procedures in use; and the roles and responsibilities for managing information to ensure compliance with legal requirements.

3 Protocol

3.1 The Council will implement information governance effectively to ensure the following:

3.1.1 **Keeping information safe and secure**

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained

3.1.2 **Recording accurately and only record what is required**

- Information will be supported by the highest quality data
- Only information that is required will be recorded

3.1.3 **Retaining and destroying records**

- Information will only be retained for as long as is required. Information will be destroyed securely as appropriate

3.1.4 **Accessible Information**

- Information will be accessible to those who have a right of access

3.2 The following ***information security principles*** guide this Protocol:

3.2.1 **Confidentiality** - Appropriate measures must be taken to ensure that information held by the Council is only accessible to those authorised to have access.

3.2.2 **Integrity** – The accuracy and completeness of information must be maintained and all changes or modifications affecting that information must be authorised, controlled and validated.

3.2.3 **Quality** - The Council must ensure that the information it holds is fit for its intended purpose.

3.2.4 **Availability** – Information must be available to authorised individuals when required. In the event of a disaster or malicious attack, the Council's information and systems critical to the operation of key services and ongoing activities must be recoverable.

3.2.5 **Authentication** – Any person or system seeking access to Council information or networks must first establish their identity to the satisfaction of the Council.

3.2.6 **Access control** – Access to view or modify information or systems must be restricted to those whose job functions specifically require such access.

3.2.7 **Auditing** – User access and activity on each of the Council's computers, firewalls and networks must be recorded and maintained in compliance with security, retention and all legislative and regulatory requirements.

3.3 The Council will monitor this guidance document, and will update it as necessary.

4 Legislation and Standards

4.1 The following legislation and standards are an integral part of the regulatory environment within which the Council must operate:

- The GDPR;
- Data Protection Act 2018;
- Freedom of Information Act 2000
- Human Rights Act 1998
- Environmental Information Regulations 2004
- Local Government Act 1972
- Computer Misuse Act 1990
- Payment Card Industry Data Security Standard

5 Roles and responsibilities

5.1 The following roles and responsibilities underpin effective Information Governance within the Council.

5.2 **Senior Information Risk Owner (SIRO)**

This role provides senior leadership for information governance in the organisation. The role:

- Ensures effective governance arrangements are in place for improving the management of information in the Council;
- Oversees the development of policies, procedures and guidance;
- Identifies organisation-wide information management risks and ensures appropriate action to mitigate risks are agreed and implemented;
- Ensures effective training and staff development is in place;
- Oversees any communications needed about information governance;

- Provides an annual report and updates as required to Corporate Management Team about the delivery and success of the information governance action plan.

5.3 **Assistant Directors / Directors**

5.3.1 Are accountable for the implementation of Information Governance, policies, procedures and guidelines in their service area.

5.3.2 Take ownership of the information in their service area.

5.3.3 Are accountable for identifying and effectively managing the information necessary for service delivery.

5.4 **Heads of Service**

5.4.1 Ensure that staff in their team(s) are aware of policies, procedures and guidance for Information Governance.

5.4.2 Ensure that the practice of managing information in their service area complies with policies, procedures and guidance.

5.4.3 Must ensure staff in their team(s) report breaches in data protection to the Council's Data Protection Officer

5.4.4 Identify risks in managing information in their service area and ensure these are mitigated and/or escalated as required

5.4.5 Ensure that members of staff attend relevant and appropriate training.

5.5 **Data Protection Officer**

5.5.1 To inform and advise the Council and its staff who carry out processing of their obligations pursuant to the GDPR.

5.5.2 To monitor compliance with the GDPR and the DPA and with the Data Protection Policy and other Data Protection Policies and Procedures.

5.5.3 To act as the contact point for the Information Commissioner's Office on all matters relating to data protection and to fully cooperate with this body.

5.6 **All Staff (whether permanent or temporary) and others using Council systems or information**

5.6.1 Have a responsibility to ensure that they are familiar with the contents of this Policy and to ensure information is managed in line with Information Governance policies, procedures and guidelines;

5.6.2 Must report breaches of data protection to their Manager;

5.6.3 Are to undertake training and support as required.

6 Training and Guidance

6.1 All Information Governance related guidance and procedures are published on the Council's intranet and available to all staff. Staff are made aware of these procedures through well-established management and communication channels – such as check ins and PDRs, team meetings, training, staff communication channels and communications campaigns. All employees are required to complete the mandatory e-learning module on GDPR.

7 Incident Management:

7.1 Clear guidance on incident management procedures should be documented and staff should be made aware of their existence, where to find them and how to implement them.

7.2 See Procedure for Reporting Information Security Breaches, Data Protection Breaches and Card Data Security Incidents www.southkesteven.gov.uk/CHttpHandler.ashx?id=24185&p=0 for further information.

This page is intentionally left blank

South Kesteven District Council

Procedure for reporting information security breaches, data protection breaches and card data security incidents

December 2020

Introduction
This procedure applies to all staff and elected Members working for the South Kesteven District Council (The Council) and it applies to any actual, suspected or "near miss" loss of personal data.

Any loss of confidential information can result in large fines for the Council. The Council is under a duty to report certain types of breaches so it is imperative that these are reported as soon as possible.

This procedure should be used to report all breaches of confidentiality and information security whether actual or suspected. This covers information held and shared in different formats (paper, electronic or verbal).

This procedure underpins the Council's Information Governance guidance, www.southkesteven.gov.uk/CHttpHandler.ashx?id=24184&p=0 and our Data Protection Policy www.southkesteven.gov.uk/CHttpHandler.ashx?id=24182&p=0 which have been developed to protect the information handled by the Council. In addition, it supports the guidelines produced for connecting to the Government Secure Internet and is part of the Council's Payment Card Industry Governance.

All staff and Elected Members have a responsibility to report a suspected or actual breach of confidentiality or loss of data. Failure to do so may be considered a breach of the Council's Data Protection Policy and may result in disciplinary action. Where there is a risk that Credit or Debit Card information may have been compromised, the Card Data Security Incident Response Plan, at Page 9 of this document, should also be followed.

Procedure
If you suspect an information security breach has occurred, you should report it immediately to the Council's Data Protection Officer (the DPO) as the Council is under a duty to report serious incidents within **72 hours** of becoming aware of them.

Breaches should be reported to dpo@southkesteven.gov.uk Telephone Number: 01476 406080. The DPO will conduct an initial investigation and risk assessment to ascertain the nature and seriousness of the incident. It is imperative that this assessment is done without delay.

If a breach meets the notification requirements, the DPO shall inform the Chief Executive of this fact. They will also inform the Information Commissioner as soon as possible and no later than 72 hours from the time the Council became aware of the breach. See Page 4 for guidance on this.

The DPO does not need to have full details of the breach available prior to making a notification to the Information Commissioners Officer (ICO). If the DPO believes, on initial assessment, that there is a likelihood that the breach will meet the notification requirements then the DPO should make the initial notification within 72 hours and update the ICO as and when further information becomes available.

The DPO will maintain a record of incidents, including a risk assessment, the outcomes and resulting recommendations made.

Breach Management Team
The Council's DPO will, if they consider it necessary, chair a breach management team to assist in responding to a breach. The exact makeup of this team will depend on the nature and the seriousness of the breach and what skills and resources are required to respond.

The core team should comprise representatives from IT Services, Legal Services, Risk & Audit, Human Resources and Communications as well as representatives from the effected service area(s). The makeup of the team will depend on the exact nature of the breach.

Guidance

What is a personal data breach?

Breaches can be categorised according to the following three well-known information security principles:

- **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.
- **Integrity breach** - where there is an unauthorised or accidental alteration of personal data.

A breach may involve a combination of these elements.

Assessing Risk and High Risk

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the ICO is only triggered where a breach is likely to result in a 'risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a 'high risk to their rights and freedoms'.

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. This includes loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include other significant economic or social disadvantage to those individuals.

A breach will be considered to pose a high risk to the rights and freedoms of individuals where the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation.

When the breach involves special category, personal data that reveals racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, or trade union membership, or includes genetic data and biometric data for the purpose of identifying a natural person, data concerning health or data concerning sex life or sexual orientation, or criminal convictions and offences or related security measures, it should be assumed that there will be a high risk to the rights and freedoms of individuals.

Factors to take into account

- Nature of the breach
- Nature, sensitivity and volume of the data
- Ease of identification
- Severity of consequences for data subject(s) - for instance identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm

- If there has been a loss of confidentiality is the 3rd party "trusted"? - The fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the ICO, or to the affected individuals.
- Special characteristics of the individual (children, vulnerable adults etc.) • The number of affected individuals

Notification of a personal data breach

1 Notifying the ICO

The GDPR and Data Protection Act 2018 makes it mandatory for serious data breaches to be reported to the ICO.

Where a breach is likely to result in a risk to the rights and freedoms of natural persons, a notification to the ICO should be made within **72 hours** of the Council (not the DPO) becoming aware of the breach.
Where a notification to the ICO is not made within 72 hours, it shall be accompanied by written reasons for the delay.

The notification needs to:

(a) Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
(b) Communicate the name and contact details of the DPO or other contact point where more information can be obtained;
(c) Describe the likely consequences of the personal data breach;
(d) Describe the measures taken or proposed to be taken by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible to provide all the above information at the same time, it may be provided in phases without undue further delay.

The Council is required to record the following information in relation to a personal data breach:

(a) The facts relating to the breach,
(b) Its effects,
(c) The remedial action taken.

It must be recorded in such a way as to enable the ICO to verify compliance.

2 Notifying data subjects affected by the breach

The Council is also required to communicate a breach to the affected individuals where the breach is likely to result in a high risk to the rights and freedoms of natural persons.
This a higher risk level than notification to the ICO.
Where a breach poses a high risk, the Council should communicate the personal data breach to the data subject without undue delay.
The communication shall describe in clear and plain language:

(a) A description of the nature of the breach;
(b) The name and contact details of the DPO or other contact point where more information can be obtained;
(c) The likely consequences of the personal data breach;

(d) The measures taken, or proposed to be taken, by the Council to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3 Circumstances where notification of the data subject is not required:

(a) When the data is protected, measures that render personal data unintelligible or inaccessible to any person who is not authorised to access it.
(b) Immediately following a breach, the Council has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise.
(c) It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. Instead, the Council must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner.

4 The Council may restrict, wholly or partly, the provision of information to the data subject by way of notification to:

(a) Avoid obstructing an official or legal inquiry, investigation or procedure;
(b) Avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
(c) Protect public security;
(d) Protect national security;
(e) Protect the rights and freedoms of others.

Card Data Security Incident Response Plan

Scope
This plan applies to all staff and contractors working for the Council.

Purpose
To address cardholder data security, the major card brands (Visa, MasterCard, etc.) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants document an incident response plan.

Any compromise of cardholder data can result in large fines for the Council and reputational damage. All staff have a responsibility to protect cardholder data.

This procedure should be used to report all incidents, whether actual or suspected. This covers information held and shared in different formats (paper, electronic or verbal).

The procedure underpins the Council's Information Governance Policy and Data Protection Policy, which have been developed to protect the information handled by South Kesteven District Council.

A data compromise, or breach, occurs when a person accesses the Council's customer's information with the intent to commit fraud. The information most valuable to criminals include the customer's card number, expiry date, name, address and the security details such as CVC / CVV code and the track data. A cardholder data compromise is any situation where theft or suspected theft of cardholder data has occurred.

Criminals may access cardholder data in a number of ways including:

- Theft from premises of terminals and terminal receipts,
- A dishonest member of staff accessing and passing on cardholder data to criminals,
- A criminal tampering with a card terminal and skimming data, • Through the Council's third party payment providers.

Procedure

If you suspect an information security breach has occurred, you should report it immediately to your line manager and / or your Business Manager.

- Have specific technical controls in place within the Contact Centre as well as governance and training in relation to processing card payments.
  If a card terminal has (or is suspected to have been) tampered with, unplug the device and Contact the IT service desk. They will collect the terminal. IT Services can provide spare CAPITA terminals and the Control Accounting Team can arrange for a replacement Global Pay terminal (contact details below).

Business Managers must report the incident to:

- The Control Accounting Team
  The Control Accounting Team will immediately inform the Relationship Manager for the Council's Merchant Services Provider and ensure the payment brands are advised within the necessary timescales. If a card terminal has been stolen or compromised, the Control Accounting team will follow the UK Cards Association procedures.

The Control Accounting Team will inform the Council's:

- Data Protection Officer, dpo@southkesteven.gov.uk, who will liaise with the IT team, and instigate any necessary remedial action.
  The Council's Data Protection Officer will maintain a record of incidents, the outcomes and any recommendations made.

In Addition

To minimise further data loss, and preserve evidence to facilitate the investigation process, the Council will not:

- Access, alter or delete files in the compromised system(s)
- Attempt to change passwords on the compromised system(s).
- Log in as administrators - indeed logon at all.
- Turn (back) on the compromised system(s).

Any logs generated are kept for at least six months in keeping with HMG GPG13.

While no system is 100% secure, South Kesteven District Council:

- Carry out active scans for credit and debit card data on any data stored and transmitted via email, and prevent this from onwards transmission.
- Have controls on USB's being added to computers, which makes the movement of skimming of data more difficult from Council computer systems.
- Only employ 3rd party payment providers who are PCIDSS compliant and listed on the Visa Europe Member or Merchant Agent Web listing.
- Ensure staff are trained in awareness in relation to card terminal tampering.

- Have specific technical controls in place within the Contact Centre as well as governance and training in relation to processing card payments.

This page is intentionally left blank

South Kesteven District Council

Procedure for undertaking a data protection impact assessment

December 2020

1 Introduction

1.1 Under previous legislation, the carrying out of a Data Privacy Impact Assessment (DPIA) was good practice. Completing a DPIA is now mandatory in certain circumstance in both the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). If you are introducing, changing, or assessing a process that handles personal data, you must complete a DPIA. This is a key element of the new focus on accountability and data protection by design, and a more risk-based approach to compliance.

1.2 A DPIA is a process to help identify and minimise the data protection risks of a particular project or activity when the processing of personal data is likely to result in 'high risk to individuals rights or freedoms'. A high risk might arise if the Council is intending to process data that:

- Involves the use of special category (sensitive), or highly personal data;
- Concerns vulnerable adults or children;
- Involves preventing people from using a service or exercising a right;
- Includes processing data on a large scale.

1.3 If you are in any doubt as to whether you need to complete a DPIA, you should consult with South Kesteven District Council's Data Protection Officer. Email: dpo@southkesteven.gov.uk

1.4 If you identify a high risk and you cannot mitigate that risk, you must consult with the DPO who will contact the Information Commissioner's Office (ICO) before starting the processing. The ICO will give written advice within 8 weeks, or 14 weeks in complex cases. In appropriate cases, the ICO has the power to issue a formal warning not to process the data, or to ban the processing altogether.

2 When should a DPIA be undertaken?

2.5 A DPIA is a process to systematically analyse the Council's processing and help SKDC to minimise data protection risks. It is intended to be an ongoing process; it should be monitored and reviewed as necessary. A DPIA must:

- Describe the processing and its purposes;
- Assess necessity and proportionality;
- Identify and assess risks to individuals; and
- Identify any measures to mitigate those risks and protect the data.

2.6 The GDPR states that the Council must carry out a DPIA if it plans to:

- Systematically monitor a public place on a large scale by for example, installing CCTV cameras;
- Process special category data or criminal offence data on a large scale;
- Use systematic and extensive profiling with significant effects;
- Use new technologies, process biometric data (e.g. fingerprints, facial recognition, retinal scans) and geometric data (an individual's gene sequence);
- Profile children or target services at them;
- Match data or combine data sets from different sources;
- Process personal data without providing a privacy notice directly to an individual;

- Process personal data that might endanger an individual's health or safety in the event of a security breach.

2.3 The GDPR also provides that the Council must, where appropriate, seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

The following checklist will assist you in terms of determining whether DPIA must be carried out.

		DPIA questions	**Yes/No**
1.	**Identity**	Will the project involve collecting information about individuals for the first time?	
2.	**Identity**	Will your project or activity compel individuals to provide information about themselves?	
3.	**Sharing information**	Will any information about individuals be disclosed to any other organisations?	
4.	**Data**	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
5.	**Data**	Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition or CCTV cameras?	
6.	**Data**	Will the project result in you making decisions or taking action against individuals in ways that could have a significant impact on them?	
7.	**Data**	Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.	
8.	**Data**	Will the project or activity require you to contact individuals in ways that they may find intrusive?	

If you have answered YES to ANY of the questions in the checklist, you will need to consult with the DPO.

3 What should a DPIA contain?

3.1 Section 64 of the DPA 2018 prescribes that a DPIA must contain as a minimum:

3.2 A systematic description of the proposed processing and its purpose;

3.3 An assessment of the risks to the rights and freedoms of data subjects;

3.4 The measures proposed to address those risks;

3.5 Safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Council's revised Data Protection Policies and Procedures.

The Data Protection Impact Assessment Template can be found on Monty or requested from the DPO and should be used when carrying out a DPIA.

South Kesteven District Council

Protocol for protecting personal information

December 2020

The Council has a duty to protect the information it holds about individuals.

Breaches of the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) can result in enforcement action being taken against the Council by the Information Commissioner's Office (ICO), and a fine of up to 20 million Euros being imposed. This in turn can lead to disciplinary action being taken against individual members of staff responsible for the data breach.

For protecting personal and special category data:

- Always keep personal information safe and secure
- Check who you are sharing information with
- Use email carefully and responsibly
- Do not store personal data on desktops and mobile devices
- Keep data secure when working away from the office
- Take extra care when taking information out of the office
- Always report information security breaches

1 Always keep personal information safe and secure

- Always ensure that records containing personal and special category data are stored securely to prevent unauthorised access. If you have paper records you must store these in a locked cabinet or drawer. You can see the definition of personal and special category data in the Council's Data Protection Policy www.southkesteven.gov.uk/CHttpHandler.ashx? id=24182&p=0
- Do not use the hard drive (the C: drive) on your desktop computer or laptop for saving and storing personal data. This is not secure and back-up copies of records are not made by IT networks.
- Never share any of your IT system passwords with anyone else. Passwords should not be written down. Passwords should be a minimum of 8 characters in length, and use a mix of letters, numbers and special characters. Do not use the same password for different systems.
- Ensure that your desk and computer cannot be overlooked by members of the public. Where you are processing special category personal information you should also consider whether care should be taken to prevent other members of staff from seeing the work.
- Be security aware when entering or leaving the office. Do not let unauthorised persons into the building. If someone asks to be let into the office or tries to follow you through the secure doors, politely ask to see their ID.
- When records no longer need to be kept (in line with the Council's Retention Schedule). All personal information held in hard copy should be disposed of appropriately using the confidential waste bins provided.
- When using the printer, photocopier or scanner please check that all documents are collected when you have finished. Check that the documents you pick up are the correct ones.
- Before sending a letter always check that the address is correct and that it is addressed to the correct recipient. Double-check any documents that are being enclosed to make sure they are the correct ones.
- You must only use authorised Council USB memory sticks. The use of any other device with Council equipment risks damaging systems. Contact your Business Support team or the IT Service Desk for assistance with this.

2 Check who you are sharing information with

- If you are sharing personal and/or special category data, you must make sure that the person you are sharing the data with has a lawful bases and right to have access to the data.

- Be careful about sharing information via the telephone. Take simple steps to verify the caller's identity to establish their identity.
- Requests for disclosure by law enforcement agencies should be made in writing.
- Members of staff must only access personal information and systems where it is necessary for their role. **Remember** - it is a disciplinary offence to use or access the Council's records for your own purposes.
- Do not discuss or share Council-owned personal data via social media. Only authorised members of staff should use social media for Council purposes.

3 Use email carefully and responsibly

- All email for Council business must be sent using the Council's email systems. Personal email accounts must not be used for council business.
- When sending an email, care must always be taken to ensure that it has been addressed to the appropriate person and that the correct email address has been used.
- When sending bulk email, it is important to use the 'blind carbon copy' function (Bcc) to prevent the inadvertent disclosure of email addresses.
- When sending emails involving special category (sensitive) content, use simple anonymisation techniques to mitigate the risks of unauthorised or accidental disclosure. For instance, use reference numbers and initials rather than names. The intended recipient will know who the information relates to but an unintended recipient will not be able to identify the subject of the email.
- Be aware of the risks posed by spam email containing viruses and malware. Whilst the Council has good anti-virus software in place, members of staff should be alert to any email that seems odd or unusual, for instance it looks out of place, is poorly spelt, contains an offer that is too good to be true etc. If you receive a suspect email do not click on any link or open any attachment it may contain, instead report it to IT immediately.

4 Do not store personal data on laptop desktops or mobile devices

- Personal data should only be stored on the Council's secure network.
- Due care and attention should be used when working on laptops or other devices when away from your normal place of work. Make sure you cannot be overlooked and never leave your equipment unattended or lend it to a third party.
- Only use Council issued or Council approved laptops or mobile devices. In some instances, it is permitted for Elected Members and employees to use a piece of their own IT equipment. This is purely for the purposes of accessing Council e-mail and must be used in accordance with the Acceptable Use of IT Policy
- http://www.southkesteven.gov.uk/CHttpHandler.ashx?id=22433&p=0

5 Keep data secure when working away from the office

- Files, paperwork and mobile computing devices must be stored in a secure location when not in use. Store any manual records separately from your IT equipment.
- Council data should not be stored at home long term. With agile working please ensure paper documents are scanned and accessed electronically and the hard copies securely destroyed of filed at the SKDC office.
- If you are leaving the Council's employment you must return all Council owned data and equipment to the Council in good time.
- A record of any files or records taken out of the office should be kept in case they are damaged/destroyed, lost or stolen. Where possible you should avoid taking original files or records out of the office.
- The Council recognises that there are circumstances when personal information will need to be taken out of the office.

- Only transport the minimum of personal information required. Ensure that you don't leave files, equipment or bags containing Council equipment or Council personal data unattended at any time or on view in a locked vehicle.
- When travelling on public transport, extra care should be taken to ensure that bags containing personal information are not lost or stolen.
- You must ensure that any electronic media has been appropriately encrypted. Only Council owned electronic transportable media should be used.
- The password (encryption key), which provides access to information being sent by any electronic media or email, must be sent to the recipient by a different method to that by which the data has been sent.
- It is good practice to keep a record of any large-scale data transfers. The record should show what data was sent, how it was sent, and what security measures were taken. All large-scale transfers of personal data must be authorised by the Assistant Director of the information asset owner's area. If in doubt, seek legal advice from the Council's Data Protection Officer.
- Where possible you should avoid working on or discussing work involving personal or sensitive matters in a public environment. If this is not possible, care should always be taken to ensure that you are not overlooked or overheard.

6 Always report information security breaches

- All staff have a responsibility to report a suspected or actual breach of confidentiality or loss of data. Early notification of an incident can ensure that any mitigating or recovery actions can take place as soon as possible. It is better to report a suspected incident even if you are unsure if one has occurred, than not to do so.
- If you suspect an information security breach has occurred, you should report it immediately to the Data Protection Officer and your line manager.
- Breaches will be dealt with in line with the Council's Procedure for
- Reporting Information Security Breaches, Data Protection Breaches and card Security Incidents www.southkesteven.gov.uk/CHttpHandler.ashx?id=24185&p=0
- There is a statutory duty on the Council to notify the Information
- Commissioner's Office of reportable breaches within **72 hours**. Failure to do so can result in a fine of up to 10 million Euros being imposed on the Council.

SOUTH KESTEVEN DISTRICT COUNCIL

Cabinet

18 May 2021

Report of: Councillor Kelham Cooke
The Leader of the Council

Key and Non-Key Decisions taken under delegated powers

This report provides an overview of decisions taken by individual Cabinet Members since the last meeting of the Cabinet on 16 March 2021.

Report Author

Lucy Bonshor, Democratic Officer

Tel: 01476 406120

Email: l.bonshor@southkesteven.gov.uk

Corporate Priority:	Decision type:	Wards:
High Performing Council	**Administrative**	**All Wards**

Reviewed by:	Shelley Thirkell, Acting Principal Democratic Officer	28 April 2021
Approved by:	Karen Bradford, Chief Executive	10 May 2021
Signed off by:	Councillor Kelham Cooke, The Leader of the Council	10 May 2021

Recommendation (s) to the decision maker (s)

1. **It is recommended that the Cabinet notes the contents of this report.**

1.1 Since the Cabinet last met on 16 March 2021, the following Key and Non-Key decisions have been taken under delegated authority:

1.1.1 **Adoption of Modern Slavery Charter**

Non-Key decision taken by the Cabinet Member for Communities on 14 April 2021

Date decision effective: 23 April 2021

Report and decision notice attached at Appendix 1

1.2 Any decision made after the publication of the agenda will be reported at the next meeting of the Cabinet.

CABINET MEMBER DECISION

SOUTH KESTEVEN DISTRICT COUNCIL

Decision:

To approve the adoption, by South Kesteven District Council, of the Safer Lincolnshire Partnership's Modern Slavery Charter.

(1) **Details of Decision**

To seek approval for the adoption of the Safer Lincolnshire Partnership's Modern Slavery Charter.

(2) **Considerations/Evidence**

The Safer Lincolnshire Partnership is asking all its partners to adopt its Charter against Modern Slavery and Human Trafficking. The Charter, which was formally launched by the Safer Lincolnshire Partnership in January 2021, can be found at Appendix A and requires the Council to commit to having adequately trained staff and procedures in place to ensure we can effectively tackle the issues of Modern Slavery and Human Trafficking and also contribute to the wider collective effort to protect communities across Lincolnshire.

Modern Slavery is a broad term that can include:

- Forced labour – any work or services, which people are, forced to do against their will under the threat of some form of punishment.
- Debt bondage or bonded labour – the world's most widespread form of slavery, when people borrow money they cannot repay and are required to work to pay off the debt, then losing control over the conditions of both their employment and the debt.
- Human trafficking– involves transporting, recruiting or harbouring people for the purpose of exploitation, using violence, threats or coercion.
- Descent-based slavery – where people are born into slavery because their ancestors were captured and enslaved; they remain in slavery by descent.
- Child slavery – many people often confuse child slavery with child labour, but it is much worse. Whilst child labour is harmful for children and hinders their education and development, child slavery occurs when a child is exploited for someone else's gain. It can include child trafficking, child soldiers, child marriage and child domestic slavery.

- Forced and early marriage – when someone is married against their will and cannot leave the marriage. Most child marriages can be considered slavery.

South Kesteven District Council's role in preventing Modern Slavery includes:

- Ensuring staff and elected Members have a clear understanding of Modern Slavery and know how to recognise and report concerns.
- Ensuring all staff and elected Members are complying with the Council's training requirements for the safeguarding of vulnerable individuals.
- Communicating and promoting materials highlighting Modern Slavery as an issue within Lincolnshire.
- Ensuring our policies and procedures are in line with the Modern Slavery Charter and current guidance.

The Charter contains seven commitments. Officers have reviewed these and the commitments are currently being achieved or are able to be achieved within existing resources. All actions are a collective responsibility across the Authority ensuring we further embed the ethos that safeguarding is everyone's responsibility.

Appendix B to the report provides reassurance of how each commitment is being, or will be, met.

Members of Rural and Communities Overview and Scrutiny Committee were asked to review, and comment on, the attached appendices. At its meeting of 11th March 2021 the Committee recommended to the Cabinet Member for Communities that South Kesteven District Council joins with other Lincolnshire Authorities and adopts the Modern Slavery Charter.

(3) **Reasons for Decision:**

Modern Slavery forms part of the Council's responsibilities to safeguard vulnerable individuals from harm. In adopting this Charter the Council is committing to working in collaboration with other Authorities in Lincolnshire to tackle Modern Slavery in all its forms.

Conflicts of Interest

(Any conflict of interest declared by any other Cabinet Member consulted in relation to the decision to be recorded).

None

Dispensations

(Any dispensation granted by the Monitoring Officer in respect of any declared conflict of interest to be noted).

None

Decision taken by:

Name: Councillor Annie Mason
Cabinet Member for Communities

Date of Decision: **14 April 2021**

Date of Publication of Record of Decision: **15 April 2021**

Date decision effective (i.e. 5 days after the date of publication of record of decision unless subject to call-in by the Chairman of an Overview and Scrutiny Committee or any 5 members of the Council from any political groups):

23 April 2021

This page is intentionally left blank

CHARTER AGAINST MODERN SLAVERY AND HUMAN TRAFFICKING

The Safer Lincolnshire Partnership's Charter against Modern Slavery and Human Trafficking commits organisations to proactively take steps internally to tackle the issue; whilst at the same time ensuring that they are contributing to the wider collective effort to protect communities across Lincolnshire.

South Kesteven District Council will:

1. Attend and actively contribute to the Safer Lincolnshire Partnership core priority group to ensure that the objectives of the group, as set out in the Safer Lincolnshire Partnership Modern Slavery delivery plan, are met.
2. Identify staff who require training in awareness, identification and action to be taken related to suspicion or disclosures of Modern Slavery taking into account the different competence requirements of particular roles.
3. Have an effective Modern Slavery policy or procedure in place detailing how to respond to suspicion or disclosures of Modern Slavery. This will include the process for notifying Lincolnshire Police & onward action as per the Lincolnshire multi-agency Modern Slavery process.
4. Have a process for escalating concerns related to Modern Slavery where appropriate action is believed not to have occurred to protect victims of Modern Slavery.
5. Ensure information about Modern Slavery is included on its website with links to the national Victim Care Contract prime provider as well as the Modern Slavery helpline.
6. Ensure Modern Slavery resources are displayed, in different languages where relevant to local communities and are also available in alternative formats such as large print upon request.
7. Report publicly on the implementation of this Charter annually.

Version 1 – June 2020

This page is intentionally left blank

Safer Lincolnshire Partnership Modern Slavery Charter – Requirements and Responses **Appendix B**

Requirement	SKDC Response	Timeline/Responsibility
Attend and actively contribute to the Safer Lincolnshire Partnership core priority group to ensure that the objectives of the group, as set out in the Safer Lincolnshire Partnership Modern Slavery delivery plan, are met.	Protecting people from modern slavery and trafficking falls within the Council's Safeguarding responsibilities. The Deputy Safeguarding Officer represents South Kesteven District Council on this group.	**Group meets quarterly**. Feedback to Designated Safeguarding Lead to inform Cabinet Member for Communities and CMT as part of Safeguarding update. Actions disseminated to responsible Heads of Service
Identify staff who require training in awareness, identification and action to be taken related to suspicion or disclosures of Modern Slavery taking into account the different competence requirements of particular roles.	Tackling Exploitation and Modern Slavery training is a requirement for staff and Elected Members through our agreed Safeguarding Policy 2020/23. This module of e learning is available through Lincolnshire's Safeguarding Children Partnership and Safeguarding Adults Board.	**Ongoing programme.** Member Services to ensure the agreed safeguarding training for Elected Members is rolled out and completed. Heads of Service to ensure staff are appropriately trained.
Have an effective Modern Slavery policy or procedure in place detailing how to respond to suspicion or disclosures of Modern Slavery. This will include the process for notifying Lincolnshire Police & onward action as per the Lincolnshire multi-agency Modern Slavery process.	Chapter 7 of South Kesteven District Council's Safeguarding Policy is dedicated to Modern Slavery and Trafficking. This chapter provides an overview of Modern Slavery and includes information on raising concerns, making referrals and also provides links to further information. The policy is reviewed on an annual basis to ensure it remains fit for purpose.	**Annual review** or more frequent as a response to legislative or statutory guidance changes. Safeguarding officers to update policy and disseminate via Heads of Service who should ensure staff and elected Members have access to up to date policy and procedures
Have a process for escalating concerns related to Modern Slavery where appropriate action is believed not to have occurred to protect victims of Modern Slavery.	As an integral part of existing safeguarding processes information on inter-agency disputes and escalation policies is contained within the Council's Safeguarding Policy	**Annual review** or more frequent as a response to legislative or statutory guidance changes. Safeguarding officers to update policy and disseminate via Heads of Service who should ensure staff and elected Members have access to up to date policy and procedures
Ensure information about Modern Slavery is included on its website with links to the national Victim Care Contract prime provider as well as the Modern Slavery helpline.	The Council's website currently contains a limited amount of information relating to Modern Slavery. To meet this objective a review of this information and an update to reflect the latest information and guidance is underway.	**May 2021** Safeguarding and Communications Officers to work collaboratively to deliver against this action
Ensure Modern Slavery resources are displayed, in different languages where relevant to local communities and are also available in alternative formats such as large print upon request.	Resources are made available in 5 other languages via the Safer Lincolnshire Partnership. These are shared with relevant voluntary and community groups in South Kesteven and are displayed in Council buildings. When community-facing services re-open to the public a review of sites will be undertaken to ensure information is available in the most appropriate places. Alternative formats are available on requests as a matter of SKDC existing practice	**Processes already in place** for distribution and display. To be reviewed once Covid restrictions have been lifted. Community-facing teams to ensure information is available and up to date in SKDC buildings. Community Engagement staff to share information with the Voluntary and Community Sector
Report publicly on the implementation of this Charter annually.	Existing practice is that an Annual Report on Safeguarding is presented to Governance and Audit Committee and, under requirements of the Public Sector Equality Duty we also produce an Equality and Diversity Annual Position Statement. Reporting in relation to this Charter will be incorporated into these published documents.	**September 2021** and annually thereafter. Community Development Officer with responsibilities for safeguarding and equalities to prepare, present and publish the required information.

This page is intentionally left blank

SOUTH KESTEVEN DISTRICT COUNCIL

Non-key Decision

6th April 2021

Councillor Annie Mason

Cabinet Member for Communities

Adoption of Modern Slavery Charter

The Safer Lincolnshire Partnership's Charter against Modern Slavery and Human Trafficking commits organisations to proactively take steps internally to tackle the issue whilst, at the same time, ensuring that they are contributing to the wider collective effort to protect communities across Lincolnshire. This report seeks the adoption of the Charter on behalf of South Kesteven District Council.

Report Author

Carol Drury – Senior Community Development Officer

Tel: 01470 406 161

Email: c.drury@southkesteven.gov.uk

Approved for publication:	Councillor Annie Mason, Cabinet Member for Communities	6th April 2021

Recommendation (s) to the decision maker (s)

The Cabinet Member for Communities to agree to the adoption, by South Kesteven District Council, of the Safer Lincolnshire Partnership's Modern Slavery Charter.

1 The Purpose of the Report

1.1 The Safer Lincolnshire Partnership is asking all its partners to adopt its Charter against Modern Slavery and Human Trafficking. The Charter, which was formally launched by the Safer Lincolnshire Partnership in January 2021, can be found at Appendix A and requires the Council to commit to having adequately trained staff and procedures in place to ensure we can effectively tackle the issues of Modern Slavery and Human Trafficking and also contribute to the wider collective effort to protect communities across Lincolnshire.

1.2 This report sets out South Kesteven District Council's commitment to recognising and reducing risk around Modern Slavery and Human Trafficking within Lincolnshire and the proposal to adopt the Safer Lincolnshire Partnership's Charter against Modern Slavery and Human Trafficking.

1.3 Modern Slavery is a broad term that can include:

- Forced labour – any work or services, which people are, forced to do against their will under the threat of some form of punishment.
- Debt bondage or bonded labour – the world's most widespread form of slavery, when people borrow money they cannot repay and are required to work to pay off the debt, then losing control over the conditions of both their employment and the debt.
- Human trafficking– involves transporting, recruiting or harbouring people for the purpose of exploitation, using violence, threats or coercion.
- Descent-based slavery – where people are born into slavery because their ancestors were captured and enslaved; they remain in slavery by descent.
- Child slavery – many people often confuse child slavery with child labour, but it is much worse. Whilst child labour is harmful for children and hinders their education and development, child slavery occurs when a child is exploited for someone else's gain. It can include child trafficking, child soldiers, child marriage and child domestic slavery.
- Forced and early marriage – when someone is married against their will and cannot leave the marriage. Most child marriages can be considered slavery.

1.4 South Kesteven District Council's role in preventing Modern Slavery includes:

- Ensuring staff and elected Members have a clear understanding of Modern Slavery and know how to recognise and report concerns.
- Ensuring all staff and elected Members are complying with the Council's training requirements for the safeguarding of vulnerable individuals.
- Communicating and promoting materials highlighting Modern Slavery as an issue within Lincolnshire.
- Ensuring our policies and procedures are in line with the Modern Slavery Charter and current guidance.

1.5 The Charter contains seven commitments. Officers have reviewed these and the commitments are currently being achieved or are able to be achieved within existing resources. All actions are a collective responsibility across the Authority ensuring we further embed the ethos that safeguarding is everyone's responsibility.

1.6 Appendix B provides reassurance of how each commitment is being, or will be, met.

1.7 Members of Rural and Communities Overview and Scrutiny Committee were asked to review, and comment on, the attached appendices. At its meeting of 11th March 2021 the

Committee recommended to the Cabinet Member for Communities that South Kesteven District Council joins with other Lincolnshire Authorities and adopts the Modern Slavery Charter.

2 Available Options Considered

2.1 No other options were considered as part of this process.

3 Preferred Option

3.1 Not applicable.

4 Reasons for the Recommendation (s)

4.1 Modern Slavery forms part of the Council's responsibilities to safeguard vulnerable individuals from harm. In adopting this Charter the Council is committing to working in collaboration with other Authorities in Lincolnshire to tackle Modern Slavery in all its forms.

5 Financial Implications

5.1 There are no financial implications associated with this decision.

Financial Implications reviewed by: Alison Hall-Wright, Head of Finance

6 Legal and Governance Implications

6.1 The charter and the Council's input to delivering its objectives fit with the council's safeguarding obligations and is to be welcomed.

Legal Implications reviewed by: Shahin Ismail Director of Law and Governance

7 Equality and Safeguarding implications

7.1 The formal adoption of this Charter will complement existing policies and procedures and ensure the Council has a strong, collaborative, foundation to safeguard vulnerable individuals and ensure equitable service.

8 How will the recommendations support South Kesteven District Council's declaration of a climate emergency?

8.1 Not applicable to this decision

9 Appendices

9.1 Appendix A – Modern Slavery Charter

9.2 Appendix B – Response Table

10 Background papers

None.

Report Timeline:	Date decision due to be made	14 April 2021
	Call-in deadline	22 April 2021
	Date decision effective (subject to call-in)	23 April 2021

This page is intentionally left blank

SOUTH KESTEVEN DISTRICT COUNCIL

Cabinet

18 May 2021

Report of: Councillor Kelham Cooke
The Leader of the Council

Cabinet Forward Plan for the period 1 June 2021 to 31 May 2022

This report highlights matters on the Cabinet's Forward Plan for the period 1 June 2021 to 31 May 2022.

Report Author

Lucy Bonshor, Democratic Officer

Tel: 01476 406120

Email: l.bonshor@southkesteven.gov.uk

Corporate Priority:	Decision type:	Wards:
High Performing Council	**Administrative**	**All Wards**

Reviewed by:	Shelley Thirkell, Acting Principal Democratic Officer	28 April 2021
Approved by:	Karen Bradford, Chief Executive	10 May 2021
Signed off by:	Councillor Kelham Cooke, The Leader of the Council	10 May 2021

Recommendation (s) to the decision maker (s)

1. **It is recommended that the Cabinet notes the contents of this report.**

1.1 The Local Authorities (Executive Arrangements) (Meetings and Access to Information) (England) Regulations 2012 set out the minimum requirements for publicity in connection with Key Decisions. The Council meets these legislative requirements through the monthly publication of its Forward Plan.

1.2 Cabinet may also receive reports on which it is asked to make recommendations to Council or review the contents and take necessary action. These items are also listed on the Forward Plan.

1.3 To help Cabinet understand what issues will be put before it in the longer-term, items for consideration during the preceding year have been included in the Cabinet's Forward Plan. The Forward Plan also includes details of items scheduled for each of the Council meetings due to be held within the plan period.

1.4 The Forward Plan for 1 June 2021 to 31 May 2022 is attached at Appendix 1.

SOUTH KESTEVEN DISTRICT COUNCIL

CABINET FORWARD PLAN
Notice of decisions to be made by Cabinet
1 June 2021 to 31 May 2022

At its meetings, the Cabinet may make Key Decisions and Non-Key Decisions. It may also make recommendations to Council on matters relating to the Council's budget or its policy framework.

A Key Decision is a Cabinet decision that is likely:

1. To result in the District Council incurring expenditure which is, or the making of savings which are, significant having regard to the District Council's budget for the service or function to which the decision relates (for these purposes, South Kesteven District Council has agreed £200,000 as the threshold at which a decision will be considered significant); or
2. To be significant in terms of its effects on communities that live or work in an area comprising two or more wards.

A Non-Key Decision is one that is not a Key Decision.

The Forward Plan

The Cabinet Forward Plan is a rolling, 12-month plan that will be updated on a regular basis. It includes those matters that are scheduled to be considered by Cabinet during the plan period. This plan also includes details of those decisions that are due to be made by the full Council.

Overview and Scrutiny

The Forward Plan will be circulated to all Overview and Scrutiny Committees and be considered at each meeting as Members set the Overview and Scrutiny Committee work programmes. Scrutiny members will be able to pick from the Forward Plan, those items relevant to their remit that they wish to scrutinise.

Notice of future Cabinet decisions and recommendations to Council

Summary	Date	Action	Contact
Housing Complaints Policy - Key Decision			
A Housing Customer Feedback Policy, which sets out how the Council will manage complaints, compliments and comments.	15 Jun 2021	To approve the policy	Cabinet Member for Housing and Planning (Councillor Robert Reid) Senior Housing and Policy Strategy Officer **Tel:** 01476 40 60 80 **E-mail:** c.bowen@southkesteven.gov.uk
Distribution of monies received by the Council under a s106 Agreement and grant of new lease and building licence at Empingham Road Playing Fields, Stamford – Key Decision			
To agree the distribution of s.106 funds and the granting of a lease and building licence at Empingham Road Playing Fields, Stamford	15 Jun 2021	To approve the distribution of s.106 funds and the granting of the lease and building licence	The Leader and Cabinet Member for Corporate Services and Property (Councillor Kelham Cooke) Director of Housing and Property **Tel:** 01476 40 60 80 **E-mail:** andrew.cotton@southkesteven.gov.uk
Disposal of land Stamford - Key Decision			
To seek approval to dispose of land at Stamford	15 Jun 2021	To approve the disposal of land	The Leader and Cabinet Member for Corporate Services and Property (Councillor Kelham Cooke) Director of Housing and Property **Tel:** 01476 40 60 80 **E-mail:** andrew.cotton@southkesteven.gov.uk

Summary	Date	Action	Contact
Proposals for Deepings Leisure Centre Development - presentation of feasibility work including options explored and operational business plans - Key Decision			
To agree the facility mix and associated capital envelope of the development to be taken forward to the next stage	Jul 2021	To approve proposals	Deputy Leader and Cabinet Member for Growth and Leisure (Councillor Barry Dobson) Head of Leisure **Tel:** 01476 40 62 39 **E-mail:** karen.whitfield@southkesteven.gov.uk
Rectory Farm - Development Brief - Key Decision			
To consider the Rectory Farm Supplementary Planning Document following consultation on a draft document	Jul 2021	To approve a Supplementary Planning Document in respect to Rectory Farm	Cabinet Member for Housing and Planning (Councillor Robert Reid) Special Projects Manager **Tel:** 01476 40 61 64 **E-mail:** p.moore@southkesteven.gov.uk
Design Guide Supplementary Planning Document - Final - Key Decision			
To consider the Design Guide Supplementary Planning Document following public consultation	Sep 2021	To approve the Design Guide Supplementary Planning Document	Cabinet Member for Housing and Planning (Councillor Robert Reid) Interim Head of Planning **Tel:** 01476 40 60 80 **E-mail:** jeff.upton@southkesteven.gov.uk
Housing Asset Management Strategy 2021-2026 - Key Decision			
To consider the strategy	Nov 2021	To adopt a Housing Asset Management Strategy	Cabinet Member for Housing and Planning (Councillor Robert Reid) Interim Assistant Director of Housing **Tel:** 01476 40 60 80 **E-mail:** chris.stratford@southkesteven.gov.uk

Summary	Date	Action	Contact
Council Tax Base 2022/23 - Key Decision			
To determine the Council Tax base to form the basis of the 2022/23 budget proposals to be recommended to Council	Dec 2021	To agree the Council Tax base 2022/23 which will form the basis of the budget proposals for the year	Cabinet Member for Finance and Resources (Councillor Adam Stokes) Interim Director of Finance, Section 151 Officer **Tel:** 01476 40 63 75 **E-mail:** r.wyles@southkesteven.gov.uk
Draft Budget Proposals for 2022/23 - Key Decision			
To consider draft budget proposals for 2022/23	Dec 2021	To agree draft budget proposals for 2022/23 for consultation	Cabinet Member for Finance and Resources (Councillor Adam Stokes) Interim Director of Finance, Section 151 Officer **Tel:** 01476 40 63 75 **E-mail:** r.wyles@southkesteven.gov.uk
Proposed Development brief for Land at Stamford North - Key Decision			
To consider the proposed development brief for land at Stamford North prior to consultation	Date to be confirmed	To approve the draft Supplementary Planning Document in respect of land at Stamford North for consultation	Cabinet Member for Housing and Planning (Councillor Robert Reid) Interim Head of Planning **Tel:** 01476 40 60 80 **E-mail:** jeff.upton@southkesteven.gov.uk