Borough Council of
King's Lynn &
West Norfolk

REPORT TO CABINET

DATE OF MEETING	9 June 2026
REPORT TITLE	Data Protection Policy 2026
LEAD MEMBER	Cllr A Beales, Leader
LEAD OFFICER	Tom Darling-Fernley, Senior Corporate Governance Officer
CONSULTEES	Executive Leadership Team
WARDS AFFECTED	n/a

KEY DECISION	NO
DECISION MAKER	Cabinet
IS THE REPORT OPEN OR EXEMPT	OPEN

FINANCIAL IMPLICATIONS	YES
HR IMPLICATIONS	YES
POLICY IMPLICATIONS	YES
STATUTORY IMPLICATIONS	YES
RISK MANAGEMENT IMPLICATIONS	YES
ENVIRONMENTAL IMPLICATIONS	NO
EQUALITY IMPACT ASSESSMENT COMPLETED	Pre-screening completed. Full EIA not required, see section below.

SUMMARY OF REPORT

The Council's Data Protection Policy was last revised in June 2024. This report presents a substantially revised Policy for Cabinet approval. The revision responds to the Data (Use and Access) Act 2025 ("DUAA"), which introduces a statutory requirement, taking effect on 19 June 2026, for the Council to have a published data protection complaints procedure in place. The revised Policy also updates and restructures the document to reflect the current legal landscape, to align with the Council's standard policy document layout, and to reflect changes to the Council's information governance structure since the 2024 edition. There are no direct financial implications arising from this report.

RECOMMENDATIONS

Cabinet resolves to:

1. Approve the Data Protection Policy 2026 at Appendix A, to take effect from the date of this meeting.

2. Note that the data protection complaints procedure required under section 103 of the Data (Use and Access) Act 2025 (inserting section 164A into the Data Protection Act 2018) will be published on the Council's website by 19 June 2026 in accordance with the statutory deadline.

3. Authorise the Data Protection Officer, in consultation with the Leader of the Council to update the Policy between formal review cycles where required by changes to ICO guidance or legislation, subject to those updates being reported to the next available Cabinet meeting.

REASON FOR DECISION

The Council has a statutory obligation to comply with UK GDPR, the Data Protection Act 2018, and from 19 June 2026 the data protection complaints procedure requirement introduced by the Data (Use and Access) Act 2025. The existing policy predates the DUAA and does not reflect the new complaints procedure obligation.

Approval of the revised Policy is necessary to ensure the Council is demonstrably compliant with its legal obligations by the statutory deadline, to protect individuals whose data the Council processes, and to protect the Council from the risk of regulatory enforcement action by the Information Commissioner's Office.

CORPORATE STRATEGY
How does this proposal support our Corporate Priorities Our priorities | Corporate Strategy 2023 - 2027 | Borough Council of King's Lynn & West Norfolk

Promote growth and prosperity to benefit West Norfolk	Robust data protection practice underpins the Council's commercial and economic development functions, including in relation to business support, inward investment, and the Council's commercial leisure operations, all of which involve processing personal data at scale.
Protect our Environment	No direct linkage.
Efficient and effective delivery of our services	The revised Policy supports the Council's ambition to deliver services to residents, businesses and visitors in a timely, accessible and trustworthy manner. Sound information governance is a prerequisite for effective digital and transactional service delivery.
Support our communities	The Council's community-facing services (including but not limited to housing benefit, homelessness, social prescribing and health and wellbeing programmes) involve processing sensitive personal data. This Policy ensures those activities are conducted lawfully and with the dignity of residents at the fore. The Corporate Strategy 2023–2027 explicitly lists Data Protection as a foundational corporate plan underpinning delivery of the strategic priorities.

REPORT DETAIL

1. Introduction

1.1. The Council, as a public authority, is a data controller under the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018"). The Council's Electoral Services department is also a data controller. This policy applies to both. The Council and its partners and contractors process personal data across all its service areas and are legally required to do so in accordance with data protection legislation.

1.2. The Council's Data Protection Policy sets out how personal data is collected, stored, used and protected. It applies to all officers, elected Members, contractors and any person processing personal data on the Council's behalf.

1.3. The Policy was last formally approved by Cabinet on 11 June 2024 (item CAB16). A substantially revised version is now presented for approval.

2. Background

2.1. The Council has maintained a Data Protection Policy since the introduction of the General Data Protection Regulation in May 2018. The Policy has been revised periodically: most recently in November 2023 (version 0.03) following routine review.

2.2. On 19 June 2025, the Data (Use and Access) Act 2025 ("DUAA") received Royal Assent. The DUAA amends but does not replace the UK GDPR and the DPA 2018. Most of its data protection provisions came into force on 5 February 2026. Section 103 of the DUAA inserts a new section 164A into the DPA 2018, which requires organisations to have a published data protection complaints procedure in place by 19 June 2026. This is a hard statutory deadline.

2.3. Separately, the ICO published updated guidance on handling data protection complaints in February 2026, setting out what an adequate complaints procedure must contain, including: a requirement to acknowledge complaints within 30 calendar days; a duty to investigate without undue delay; and a requirement to communicate outcomes and signpost complainants to the ICO where they remain dissatisfied.

2.4. The existing Policy predates the DUAA and does not adequately address the complaints procedure requirement. A substantive revision is therefore necessary both to achieve statutory compliance by 19 June 2026 and to bring the Policy up to date with the broader legal landscape.

2.5. The revision has also been used as an opportunity to restructure the Policy in line with the Council's standard policy document taxonomy, to update the Council's information governance role structure (replacing Information Asset Assistants with a wider network of Information Governance Leads), and to remove and cross-refer to guidance-level material that is more appropriately located in supporting procedural documents and appendices.

3. Proposal

3.1. Cabinet is asked to approve the revised Data Protection Policy 2026, at Appendix A. The key changes from the 2023 edition are as follows:

Data protection complaints procedure (new)

3.2. The most significant change is the introduction of a dedicated complaints procedure in response to section 103 of the DUAA. The procedure sets out how individuals can raise a data protection complaint with the Council, the Council's acknowledgement obligation (within 30 calendar days), the investigation and outcome process, and the route of escalation to the ICO. A complaint is broadly defined: it covers any expression of dissatisfaction about how the Council has handled personal data and does not need to reference legislation to qualify. The procedure will be accompanied by an accessible electronic complaint form to be published on the Council's website by 19 June 2026.

Updated legal framework

3.3. The Policy's legal framework section has been expanded to provide brief contextual narrative against each piece of relevant legislation, and to incorporate the DUAA.

3.4. The Regulation of Investigatory Powers Act 2000 ("RIPA") and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 have been added in light of the Council's operation of CCTV and the sharing of CCTV footage with Norfolk Constabulary under a formal Service Level Agreement.

3.5. The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR") have been given greater prominence in recognition of the Council's commercial leisure and cultural operations, which are subject to PECR's requirements around marketing communications and cookies.

Restructured to policy template

3.6. The 2023 edition did not follow the Council's standard policy document layout. The revised Policy adopts this structure, with a clear Executive Summary,

Introduction, Aims, SMART Objectives, Scope, Definitions, Legal Framework, Roles and Responsibilities, Policy provisions, Governance Arrangements, Additional Resources, and Equality, Diversity and Inclusion section.

Clear objectives (new)

3.7. The revised Policy includes four SMART objectives: establishing the complaints procedure by 19 June 2026; improving response-on-time performance for data subject access requests and freedom of information requests; increasing information governance competence through training and the IG Leads network; and improving transparency and record-keeping, including via the regularisation of Article 30 records and proactive publication of disclosures.

Information governance structure updated

3.8. The role of Information Asset Assistant has been replaced by Information Governance Lead, reflecting a broader remit: IG Leads carry heightened awareness of information governance across their service area, maintain Article 30 records, and act as first points of contact for information rights requests and data protection complaints within their teams.

Roles and responsibilities clarified

3.9. The Policy now clearly distinguishes between the accountability of the SIRO (the Chief Executive, who is accountable for information risk) and the operational responsibility of the DPO (the Corporate Governance Manager, to whom the SIRO delegates day-to-day compliance). This is consistent with the ICO's expectations for demonstrable governance structures.

Scope clarified to include non-corporate channels

3.10. The Policy now expressly addresses personal data processed by officers or Members via personal devices or non-corporate messaging platforms in the course of Council functions. Such data falls within the scope of UK GDPR and this Policy, consistent with ICO guidance on personal email and messaging accounts.

Guidance-level material relocated

3.11. Material that was previously embedded in the policy body, including detailed breach reporting steps, DPIA criteria, and FOI procedural requirements, has been streamlined in the Policy and relocated to supporting procedural documents and appendices, making the Policy itself a cleaner statement of the Council's obligations and commitments.

Appendix A (data protection principles) enhanced

3.12. The revised Appendix A sets out each of the six UK GDPR data protection principles with worked examples drawn from district council service areas, to aid officer understanding and application.

Appendix B (conditions for special category and criminal offence data) enhanced

3.13. Appendix B to the policy now links explicitly to the Council's data retention schedules to identify processing activities that engage special category and criminal offence data. More generally, this appendix together with the policy now constitute an "appropriate policy document" for the Council within the meaning of the Data Protection Act 2018.

4. Options Considered

Option 1: Approve the revised Policy (recommended)

4.1. This is the only option that achieves statutory compliance with the DUAA by 19 June 2026 and brings the Council's policy framework up to date with the current legal landscape.

Option 2: Defer approval

4.2. This would see the Council push the full policy approval back in time and publish the complaints procedure as a standalone document. It would be technically possible to publish a standalone complaints procedure to meet the 19 June 2026 deadline without revising the full Policy. However, this would leave the Policy outdated and inconsistent with the procedure and would require a further Cabinet report in the short term. It is not recommended.

Option 3: Do nothing

4.3. Failure to have a published data protection complaints procedure in place by 19 June 2026 would place the Council in breach of a statutory obligation under the DPA 2018 (as amended by the DUAA). This would expose the Council to regulatory enforcement action by the ICO, potential punitive financial penalties and reputational damage. This option is not recommended.

5. Financial Implications

5.1. The revised Policy does not give rise to any direct financial implications. The complaints procedure will be administered within existing Corporate Governance team capacity. The Council's annual ICO registration fee is already met within existing budgets.

5.2. Non-compliance with data protection legislation carries significant financial risk. The Information Commissioner is empowered as regulator to issue effective, proportionate and dissuasive penalties for infringements.

5.3. Public bodies are usually issued with reprimands but can be issued with financial penalties in the most egregious cases. Egregiousness is determined as part of assessing the seriousness of an infringement.

5.4. For failure to comply with any of the data protection principles, any rights an individual may have under DPA 2018 Part 3, or in relation to any transfers of data to third countries, a higher maximum applies, which is £17.5mn or 4% of "turnover" (whichever is higher).

5.5. For infringement of other provisions, such as administrative requirements of the legislation, a standard maximum applies, which is £8.7 million or 2% of turnover.

6. HR Implications

6.1. The revised Policy reinforces existing mandatory data protection training requirements for all officers and Members. Targeted additional training for Information Governance Leads and customer-facing teams on recognising and escalating data protection complaints will be delivered by 19 June 2026, within existing team capacity.

7. Policy Implications

7.1. The revised Policy is designed to support the Council's Corporate Strategy 2023–2027, which lists Data Protection as a foundational corporate plan. It has also been restructured to align with the Council's standard policy document structure.

7.2. It complements and should be used in conjunction with the Council's ICT Security Policy, Retention and Disposal Policy, Retention Schedules, Publication Scheme, CCTV Code of Conduct, and supporting internal procedures for information governance and data protection.

7.3. Other policy development follows on from this work, to ensure the Council is equipped with a comprehensive information governance policy suite to support its ongoing work.

8. Climate Change and Environmental Implications and considerations

8.1. NONE

9. Statutory and Legal Implications

9.1. The primary legislative framework is the UK GDPR, the DPA 2018 (as amended by the DUAA), and the DUAA itself. Section 103 of the DUAA

(inserting section 164A into the DPA 2018) creates a statutory obligation to have a published data protection complaints procedure in place by 19 June 2026.

9.2. The Council acts as data controller. Failure to comply with data protection legislation exposes the Council to enforcement action by the ICO, including fines of up to £17.5 million or 4% of annual global turnover (whichever is higher) for the most serious breaches, and to claims for compensation from affected individuals.

9.3. The Policy has been drafted by the DPO and reviewed by Legal Services.

10. Local Government Reorganisation Implications

10.1. The Council is engaged in local government reorganisation ("LGR") planning. The data protection obligations addressed by this Policy apply regardless of the LGR timeline. Compliance with the 19 June 2026 statutory deadline from the DUAA for a complaints procedure is not discretionary.

10.2. The DPO is engaged with LGR programme leads to ensure information governance arrangements are addressed within transition planning. Following the Secretary of State's "minded-to" decision, a future unitary West Norfolk Council will require new data protection policy arrangements to support its wider service remit.

11. Health and Safety Implications

11.1. NONE directly. The Policy's security provisions, including the obligation to report data breaches promptly, support the health and safety of individuals whose data the Council holds by minimising risks from unauthorised disclosure.

12. Consultees

12.1. The revised Policy has been developed by the DPO within Corporate Governance and reviewed by the Executive Leadership Team. The Leader of the Council has been briefed.

12.2. No trade union consultation is required as the Policy does not materially alter terms and conditions of employment, though the mandatory training requirements have been noted to HR.

13. Equality Impact Assessment

13.1. A pre-screening Equality Impact Assessment has been completed. No disproportionate negative impacts on any protected group have been identified. The Policy's data protection complaints procedure has been

designed to be accessible to all, with alternative submission routes (email, post, in-person via appointment with the DPO) supplementing the online complaint form to ensure no individual is excluded by reason of disability, language, or literacy. A full impact assessment is not required.

13.2. There is a need noted from CEWG review of the pre-screening below to ensure that all can access the relevant information and understand how to complain or receive assistance to complain under this policy. Suitable measures will be taken in this regard prior to the revised policy going live.

14. Risk Management Implications

14.1. The primary risk is failure to publish a compliant data protection complaints procedure by 19 June 2026, which would place the Council in breach of a statutory obligation and expose it to ICO enforcement. This risk is mitigated by Cabinet approval of the Policy at this meeting, with the complaint form and published procedure to follow by the statutory deadline.

14.2. A secondary risk is inadequate staff awareness of the new complaints procedure, leading to complaints not being recognised or escalated correctly. This is mitigated by the targeted training programme for IG Leads and customer-facing teams committed to in the Policy's objectives.

14.3. A third risk is that the ICO issues further guidance on complaints procedures following the 19 June 2026 commencement date that requires adjustments to the Council's approach. Recommendation 3 above addresses this by authorising the DPO to make non-material updates between review cycles.

14.4. Item S6 on the corporate risk register is intended to address ongoing information risk and its management.

15. Conclusion

15.1. The Data (Use and Access) Act 2025 places a hard statutory deadline of 19 June 2026 on the Council to have a published data protection complaints procedure in place. The revised Data Protection Policy 2026 meets that obligation, links to and underpins the Council’s Corporate Strategy, updates the Council's data protection framework to reflect the current legal landscape, and restructures the Policy to align with the Council's standard document template.

15.2. Cabinet is asked to approve the Policy to enable implementation ahead of the statutory deadline.

LIST OF APPENDICES
Appendix A: Proposed Data Protection Policy 2026

LIST OF BACKGROUND PAPERS

Data (Use and Access) Act 2025
ICO guidance: How to deal with data protection complaints (February 2026)
Borough Council of King's Lynn & West Norfolk Corporate Strategy 2023–2027
Extant Data Protection Policy v0.03

PRE SCREENING EQUALITY IMPACT ASSESSMENT

For equalities profile information please visit Norfolk Insight - Demographics and Statistics - Data Observatory

Name of policy/service/function	Data Protection Policy 2026			
Is this a new or existing policy/ service/function? *(tick as appropriate)*	New		Existing	☑
Brief summary/description of the main aims of the policy/service/function being screened. Please state if this policy/service is rigidly constrained by statutory obligations, and identify relevant legislation.	This policy revision aligns with Corporate Strategy, introduces a process for data protection complaints, aligns with the KLWN policy template, and rationalises the policy making it easier to follow. There is a clear legal framework around the activities described, captured in the relevant sections of both the policy and the attendant Cabinet report.			
Who has been consulted as part of the development of the policy/service/function? – new only *(identify stakeholders consulted with)*	n/a			

Question	**Answer**				
1. Is there any reason to believe that the policy/service/function could have a specific impact on people from one or more of the following groups, for example, because they have particular needs, experiences, issues or priorities or in terms of ability to access the service?		Positive	Negative	Neutral	Unsure
	Age			☑	
	Disability			☑	
	Sex			☑	
	Gender Re-assignment			☑	
	Marriage/civil partnership			☑	

Please tick the relevant box for each group. NB. Equality neutral means no negative impact on any group. ***If potential adverse impacts are identified, then a full Equality Impact Assessment (Stage 2) will be required.*** **For more information on health inequalities please visit [The King's Fund]* **For more information on health inequalities please visit [The King's Fund]*	Pregnancy & maternity			☑	
	Race			☑	
	Religion or belief			☑	
	Sexual orientation			☑	
	Armed forces community			☑	
	Care leavers			☑	
	Health inequalities*			☑	
	Other (eg low income, caring responsibilities)			☑	

Please provide a brief explanation of the answers above:

This policy update has neutral impacts on the protected characteristics listed above, with the exception of people on lower incomes. Here, there is a moderate risk to equity of access to processes. Mitigating actions are discussed later in this pre-screening.

Question	**Answer**	**Comments**
2. Is the proposed policy/service likely to affect relations between certain equality communities or to damage relations between the equality communities and the Council, for example because it is seen as favouring a particular community or denying opportunities to another?	No	There is a moderate risk arising from equity of access to the processes under this policy that support data subjects' rights.
3. Could this policy/service be perceived as impacting on communities differently?	No	

If 'yes' to questions 2 - 3 a full impact assessment will be required unless comments are provided to explain why this is not felt necessary:

Decision agreed by EWG member:
……..

4. Are any impacts identified above minor and if so, can these be eliminated or reduced by minor actions? If yes, please agree actions with a member of the Corporate Equalities Working Group and list	Yes	**Actions:** Risk under question 2 is already mitigated through use of plain English, translation services and a variety of communication media. Access and routes to these will be clarified ahead of the policy go-live.

agreed actions in the comments section		**Actions agreed by EWG member:** ……
5. Is the policy/service specifically designed to tackle evidence of disadvantage or potential discrimination?	Yes	**Please provide brief summary:**

Assessment completed by: Name	Tom Darling-Fernley		
Job title	Senior Corporate Governance Officer		
Date completed	29 April 2026		
Reviewed by EWG member	Alison Demonty 	**Date**	30 April 2026

✓ **Please tick to confirm completed EIA Pre-screening Form has been shared with Corporate Policy** (corporate.policy@west-norfolk.gov.uk)