Borough Council of
King's Lynn &
West Norfolk

Data Protection Policy

Owner	Data Protection Officer (Interim Corporate Governance Manager)		
Responsible Person	Senior Corporate Governance Officer		
Review Cycle	Two years, or on legislative change	**Next Review Date**	June 2028
Equality Impact Assessment (EIA) Date	29 Apr 2026	**Date approved by the CEWG**	30 Apr 2026
List any other impact assessments that have been completed	Not applicable		
Date approved by Cabinet			
Published to	Public		
Stakeholders consulted	Executive Leadership Team		

Revision Record		
Rev. No.	**Date of Issue**	**Reason for Revision**
1.00	May 2026	Adapting to Data (Use and Access) Act 2025 and aligning policy and procedure. Staffing changes.
0.05	Apr 2026	Rationalised bookmarks for accessibility.
0.04	Jun 2024	Cabinet approval of revised policy (11 Jun 2025 item CAB16).
0.03	Nov 2023	Review period.
0.02	Nov 2022	Review period / following UK GDPR.
0.01	May 2018	Introduction of GDPR.

Contents

1. Executive summary

1.1. This Data Protection Policy sets out how the Borough Council of King's Lynn and West Norfolk ("the Council") collects, stores, uses and protects personal data. It applies to all Elected Members, officers, contractors and any person processing personal data on the Council's behalf.

Policy at a glance:

- Lays out four time-bound objectives for improving the Council's performance in relation to data protection and information governance.
- Defines the Council's approach to people's data rights under the relevant legislation – GDPR, Data Protection Act 2018 and Freedom of Information Act 2000.
- Links data protection and information governance to the Council's Corporate Strategy as a key enabling pillar.
- Sets out our tools and timescales for responding to requests.
- Sets out a clear process for data protection complaints under new legislation – the Data (Use and Access) Act 2025.
- Sets up a network of Information Governance Leads to support their teams and respective Information Asset Owners in their execution of this policy.

2. Introduction

2.1. This policy sits within the Council's broader corporate governance framework as referenced in the Corporate Strategy 2023–2027. The strategy places data protection alongside equality and climate change part of a foundational corporate plan that enables the delivery of four strategic priorities. This policy gives operational substance to that commitment.

2.2. Sound data stewardship underpins the Council's commitment to efficient and effective service delivery. The strategy sets out an ambition to provide information to residents, businesses and visitors in a timely and accessible manner, consult meaningfully with communities, and retain a skilled, trusted workforce. This requires disciplined handling of personal data.

2.3. Equally, the Council's drive to support communities involves processing sensitive personal data at scale. This policy ensures those activities are conducted lawfully, proportionately and with the dignity of residents at the fore.

2.4. The Council's operating principles of transparency, respect and collaborative working are only credible if the organisation can be trusted with people's

information. This policy establishes clear accountability, defined retention standards, and robust individual rights processes.

2.5. The Council supports the aims and provisions of the UK General Data Protection Regulation ("UK GDPR") and the Data Protection Act 2018 ("DPA 2018") and seeks to ensure compliance with same. It also lays out the Council's response to the Digital (Use and Access) Act 2025 ("DUAA 2025"). The DUAA 2025 amends but does not replace the UK GDPR and the DPA 2018, and most of its data protection provisions came into force on 5 February 2026. The requirement for organisations to have a published data protection complaints procedure takes effect on 19 June 2026.

2.6. The Council is a data controller. The Council's Electoral Services department is also a data controller. This Data Protection Policy applies to both and references to "the Council" throughout this policy are to both controllers.

2.7. Elected Members act in their role within the Council and where they do, this policy applies to them. At other times, elected Members are data controllers in their own right. In those circumstances, they will control and be accountable for how they implement the processing of data under the legislation.

2.8. **Compliance with this policy is mandatory.** Failure to comply may expose individuals to disciplinary action or personal criminal liability, and the Council to enforcement action by the Information Commission, financial penalties and reputational damage.

3. Aims

3.1. This policy aims to:

- help Elected Members, officers and other relevant persons meet their data protection obligations under relevant legislation;
- balance the Council's need to collect and process personal data with the rights of individuals to control their information and their privacy;
- set out the principles the Council applies when processing personal data to safeguard one of its most valuable assets and do so legally;
- establish and maintain a procedure for handling data protection complaints; and
- support the Council's wider corporate objectives through responsible, transparent information management.

4. Objectives

Objective 1: Establish a clear procedure for data protection complaints

4.1. The DUAA sets out a requirement to establish and maintain a procedure for handling data protection complaints.

In time for or starting from 19 June 2026, the Council will:

- Publish a data protection complaints procedure and an accessible electronic complaint form.
- Acknowledge all data protection complaints within 30 calendar days of receipt. Investigate all complaints without undue delay, keeping complainants informed of progress.
- Communicate the outcome of every complaint, including reasons and the complainant's right to escalate to the Information Commission.
- Maintain a central, structured log of complaints with clear investigation ownership and a focus on learning outcomes with attributed actions.
- Towards the end of the 2026-27 financial year, reflect on performance so far and refine procedures and quality targets for data protection complaints.

Objective 2: Improve performance on information governance requests

4.2. The Council seeks to improve the rate of on-time response to data subject access requests (DSARs), freedom of information requests (FOIRs), and reports of potential data breaches.

The Council will:

- Respond to DSARs and other data subject rights requests within one calendar month (extendable by two months for complex requests).
- Achieve a DSAR response-on-time rate of 90% by the end of September 2026, and 95% by the end of March 2027.
- Achieve an FOIR response-on-time rate of 95% by the end of September 2026.
- Achieve a potential data breach investigation response-on-time rate of 90% by the end of March 2027.
- Achieve an on-time rate of 100% for notifications of qualifying potential breaches to the Information Commission (according to their guidance) by the end of June 2026.

Objective 3: Increase information governance competence and awareness

4.3. Information governance sits within the Council's Corporate Governance team. Capacity in this team is finite, and there is a need to propagate and diffuse relevant knowledge and ownership throughout the organisation.

The Council will:

- Publish and maintain an e-learning module on data protection with mandatory refreshers for all officers and Elected Members on an annual basis. Target 95% completion within the first quarter of each financial year.
- Establish and embed a network of information governance leads ("IG Leads") in each service area of the Council.
- Support IG Leads to maintain their heightened awareness of information governance matters above the mandatory baseline for all officers and Members, to be the go-to contact points for all requests as relevant to their respective teams, and to maintain Article 30 records and information asset registers for their teams.
- Deliver targeted training for IG Leads and customer-facing teams on recognising and escalating data protection complaints, by 19 June 2026.

Objective 4: Improve transparency, record keeping, and risk assessment

4.4. The Council's Publication Scheme, Article 30 records, information asset registers, retention and disposal policies require review and alignment. Proactive appropriate disclosure of FOIA disclosures is deemed best practice.

The Council will:

- By the end of September 2026, consider updates to the Council's 2019 Publication Scheme and validate its alignment with the Information Commissioner's model scheme.
- By the end of September 2026, consider updates and realignment of the Council's policies, schedules and toolkit relating to data retention and disposal.
- Via the network of IG Leads, regularise the approach to Article 30 records and information asset registers on a team-by-team basis, and achieve updates and full compliance by the end of June 2026.
- Up-skill IG Leads through courses, seminars and discussion and develop suitable measures of this by the end of September 2026.
- Subject to suitable limits and exemptions, publish FOIR disclosures proactively via the Council's website (or other suitable platform) by the end of March 2027.
- Where proposed processing activities are high-risk, ensure that proposals to approvers are accompanied by a complete data protection impact assessment that has been reviewed and checked by the Data Protection Officer or their nominated representative.

5. Scope

5.1. This policy applies to:

- all employees of the Council: permanent, temporary or agency; past or current;
- elected Members, in exercising their Council role;
- contractors, consultants, partners, volunteers and others acting on behalf of the Council;
- council-owned companies and entities processing data on behalf of the Council; and
- data processors engaged by the Council under written contract.

5.2. It applies to all personal data processed by or on behalf of the Council, regardless of media (including but not limited to electronic, paper, audio or visual recordings, and non-corporate communications channels) and regardless of location.

5.3. In respect of personal data processed by officers or Elected Members for work purposes via personal means (be that via physical media, devices, accounts, non-corporate messaging platforms, or any other means), this information falls within the scope of UK GDPR and this policy. The Information Commission publishes guidance on official information held in non-corporate communications channels.

6. Definitions

Article 30 record of processing activities – The mandatory record of data processing activities maintained by a data controller. For the Council, this is an aggregate of templated documents maintained on a per-service basis alongside an information asset register.

Consent – Permission by the data subject to process their personal data. The consent must be freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement, or by a clear affirmative action, signifies agreement to the processing of their personal data. Consent can be withdrawn at any time.

Criminal offence data – Information relating to a data subject's criminal convictions, offences, allegations, investigations or proceedings. Requires additional lawful basis for processing.

Data controller – The person who (either jointly or in common with other persons) determines the purposes for and the means in which any personal data is or are to be processed. NB: the Data Controller is usually a company or organisation and is not an individual within that company or organisation.

Data processor – Any third party that processes personal data on behalf of a data controller.

Data protection complaint – Any expression of dissatisfaction by a data subject about the way their personal data has been collected, used, stored, shared or otherwise processed. Covers DSAR/rights-request handling, data security (including breach impacts), accuracy, retention, and collection practices. Does not need to reference legislation to qualify.

Data subject – Any living individual who is the subject of personal data.

DSAR or data subject access request – A request made by an individual (or a person acting on their behalf) to know whether the Council holds their personal data and, if so, to receive a copy. The Council must respond within one calendar month, subject to identity verification and applicable exemptions under the DPA 2018.

DPIA or data protection impact assessment – A risk assessment prior to data processing that is likely to result in a higher risk to data subjects' rights and freedoms (UK GDPR Art. 35).

GDPR or UK GDPR – The United Kingdom General Data Protection Regulation. This is European Union law retained via the European Union (Withdrawal) Act 2018. It governs how personal data is handled in the UK.

Information asset register – A record maintained by each Directorate documenting the personal data it processes, including the purpose, lawful basis, retention period, and any third-party sharing arrangements. Maintenance of these records is a legal requirement under UK GDPR Article 30 and is the responsibility of the relevant Information Asset Owner.

Personal data – Any information relating to an identified or identifiable person. This includes information which can directly or indirectly identify the individual and can include name, identification number, location data, online identifier, or factors specific to the physical, physiological, genetic, mental economic, cultural, or social identity of that natural person.

Processing – Any treatment of personal data: it includes collecting, recording, organising, structuring storing, altering, retrieving, using, disclosing, sharing, making available as well as restricting, erasing, and destroying.

RoPA – See **Article 30 record of processing activities**

Special category data – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning sex life or sexual orientation. Requires additional lawful basis for processing.

7. Legal framework and relevant legislation

7.1. The Council's data protection obligations arise from the following primary and secondary legislation.

European Convention on Human Rights ("ECHR")
Human Rights Act 1998 ("HRA")

7.2. The HRA translates the ECHR into UK law. ECHR Article 8 (right to respect for private and family life) underpins the Council's data protection obligations and must be considered wherever the Council's processing activities engage individuals' reasonable expectation of privacy.

7.3. The Council's compliance with UK GDPR and this policy is consistent with and supports its duties under the HRA.

Data Protection Act 2018 ("DPA") / European Union (Withdrawal) Act 2018
UK General Data Protection Regulation ("UK GDPR")

7.4. Together these set out the data protection principles and govern the processing of personal data in all formats. All personal data processed by or on behalf of the Council must comply with the six data protection principles; see **Appendix A: The Personal Data Protection Principles**.

7.5. Under UK GDPR Articles 13 and 14, individuals must be informed about how their data is used. Under Articles 15 to 22, data subjects have enforceable rights including subject access, rectification, erasure, restriction, objection, and rights relating to automated decision-making and data portability.

7.6. Processing must be based on on or more lawful bases and carried out fairly and transparently. Special category and criminal offence data require

additional conditions. See **Appendix B: Processing personal data** for the conditions around processing these categories of data.

7.7. Under Article 35 UK GDPR, the Council must carry out a Data Protection Impact Assessment ("DPIA") before undertaking processing likely to result in high risk to individuals' rights and freedoms. This applies as part of the design and planning of new projects, policies, working practices, organisations, or other initiatives. See **Appendix C: Data Protection Impact Assessments** for further information on this process.

7.8. Under Article 28 UK GDPR, written contracts must be in place with all data processors, who may only be appointed where they can provide sufficient guarantees of compliance.

7.9. Under Articles 33 and 34 UK GDPR, personal data breaches likely to result in risk to individuals must be reported to the Information Commission within 72 hours. Where the risk is high, affected individuals must also be notified directly.

Data (Use and Access) Act 2025 ("DUAA")

7.10. DUAA introduces new obligations including, at §103 (which inserts §164A into the DPA 2018), a statutory requirement for the Council to have a published data protection complaints procedure in place by 19 June 2026.

Freedom of Information Act 2000 ("FOIA")

7.11. FOIA gives the public a right of access to recorded information held by public authorities, subject to defined exemptions. The Council must respond to requests within 20 working days and maintain and publish a model publication scheme.

Aarhus Convention
European Union (Withdrawal) Act 2018
Environmental Information Regulations 2004 (SI 2004/3391) ("EIRs")

7.12. EIRs give the public a right of access to environmental information, with a stronger presumption in favour of disclosure than FOIA. Requests under the EIRs arise frequently across planning, environmental health, flood risk and waste services and are subject to the same 20 working day response obligation.

Communications Act 2003
Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) ("PECR")

7.13. PECRs govern the use of electronic communications for marketing purposes and the use of cookies and similar tracking technologies. PECRs apply (for example) to the Council's commercial operations and to any Council-operated digital platforms that use non-essential cookies.

Regulation of Investigatory Powers Act 2000 ("RIPA")
Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) ("LBPRs")

7.14. RIPA governs the lawful interception of communications and the use of covert surveillance by public authorities. The Council operates closed-circuit television ("CCTV") and may in certain circumstances conduct directed surveillance in the exercise of its enforcement functions. Any such activity must be authorised in accordance with RIPA and the Council's CCTV Code of Conduct.

7.15. The LBPRs permit limited interception of business communications (such as monitoring of staff emails or calls) for defined lawful business purposes, subject to appropriate notice to users. [it policies]

7.16. The Council shares CCTV footage to support law enforcement agencies. Any disclosure of CCTV evidence must be made in accordance with a formal Service Level Agreement in line with UK GDPR and must not on an *ad hoc* basis outside its terms.

8. Roles and responsibilities

8.1. All Elected Members, officers, and any persons holding or processing personal data on behalf of the Council have a role in implementing this policy.

8.2. To help employees comply, the Data Protection Officer provides training and guidance documents. Corporate Governance provides day-to-day support for the organisation.

8.3. An e-learning module, Data Protection Essentials, is available on the Council's learning management system and is mandatory for all staff. Employees should familiarise themselves with this Policy and guidance, complete training and apply the provisions in relation to any processing of personal data.

8.4. Failure to comply with this policy could amount to misconduct, which can be a disciplinary matter and could ultimately lead to the dismissal of staff. Serious breaches could also result in personal criminal liability.

8.5. This policy continues to apply to individuals even after their relationship with the Council ends.

There are some officers who take on statutory or key roles:

Data Protection Officer ("DPO")

8.6. The DPO has a degree of autonomy within the Council, and is responsible for advising the Council, including its senior Officers and elected Members, of its obligations under the legislation. The DPO is designated based on professional qualities and expert knowledge of data protection law and practice.

8.7. The DPO monitors compliance, raises awareness, and ensures training for staff to enable them to lawfully comply with processing operations. The DPO is the contact point with the Information Commission in the event of potential data breaches and other relevant matters.

8.8. The Council must provide the DPO with the necessary resources, professional development and access to personal data and processing operations to allow them to perform their role and to maintain their expert knowledge of data protection law and practice.

8.9. The Corporate Governance Manager is designated as the DPO and works within the Chief of Staff Directorate of the Council. They are supported in

dealing with requests and queries from data subjects by the Information Governance Officer and the Corporate Governance service area.

8.10. Please contact the DPO if you have any concerns of deviation from this policy or from the relevant legislation (see contact details on page 18 below).

Senior Information Risk Officer ("SIRO")

8.11. The Chief Executive and Head of Paid Service is designated as the Council's SIRO and is accountable for the Council's information risk management. The SIRO delegates operational responsibility for data protection compliance and information risk control to the Data Protection Officer, who acts with the SIRO's authority.

8.12. The SIRO receives escalated information risk reports from Information Asset Owners to ensure that information risk is visible and considered at Cabinet level.

Information Asset Owners ("IAOs")

8.13. Each Assistant Director in the Council is an IAO, accountable for compliance with this policy for their respective Directorates and the maintenance of compliant records.

8.14. IAOs are also accountable for the management and timely disposal of records in compliance with published data retention schedules applicable to their Directorates and Service Areas.

8.15. IAOs report escalated information risks to the SIRO. They are supported day-to-day by Information Governance Leads within their teams.

Information Governance Leads ("IG Leads")

8.16. IG Leads maintain heightened awareness of information governance matters above the mandatory baseline for all officers. They are operationally responsible for the duties of Information Asset Owners with their support and guidance and act as primary contacts for all requests as relevant to their respective teams.

8.17. IG Leads ensure operational compliance with this policy for their respective Directorates and are accountable for the maintenance of compliant Article 30 records of processing activity and information asset registers.

Information Governance Officer ("IGO")

8.18. The IGO supports the Data Protection Officer in ensuring the Council is compliant with all relevant legislation and regulatory frameworks. They liaise with Directorates and Service Areas primarily via Information Governance Leads to ensure compliance. They are responsible for processing, recording and facilitating responses to requests and notifications under the relevant legislation, and liaising as necessary with the Information Commission.

8.19. Please contact the IGO in the first instance with questions about the operation of this policy or the relevant legislation (see contact details on page 18 below).

Information Commission ("Commission")

Note: Under the Data (Use and Access) Act 2025, the Information Commissioner as a "corporation sole" will be replaced by an Information Commission constituted as a board with a non-executive chair. This change was imminent at the time of writing. This policy refers throughout to the Information Commission and should be read as referring to both terms.

8.20. As the independent regulator responsible for enforcing the relevant legislation, the Commission has broad investigatory and corrective powers. It can issue fines, enforcement notices and, in serious cases, prosecute individuals who commit criminal offences under the DPA 2018.

8.21. The Council is required to register with and pay the applicable fee to the Commission annually. Officers and Members must be aware that non-compliance may expose both the Council and individuals personally to regulatory action.

8.22. People who are unsatisfied with the Council's responses to any data protection complaint or requests under the relevant legislation are entitled in law to escalate their issues to the Commission.

> Web: **ico.org.uk**
>
> Telephone: **0303 123 1113** (Mon to Fri 9am to 5pm)
>
> Post: Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
> (note: this office will relocate to Manchester in Autumn 2026)

9. Policy

Data protection principles

9.1. All personal data processed by or on behalf of the Council must comply with the six data protection principles set out in UK GDPR Article 5. See **The Personal Data Protection Principles**

9.2. for details of the principles.

Lawful basis for processing

9.3. Processing must be based on at least one lawful basis under UK GDPR Article 6.

9.4. Processing of special category data requires an additional condition under Article 9. Processing of criminal offence data requires an additional condition under Article 10 and, in most cases, Schedule 1 of the DPA 2018. Both the lawful basis and any additional condition must be identified and documented before processing commences.

9.5. See **Appendix B: Processing personal data** for details of the lawful bases and the additional conditions and schedules.

Data subject rights

9.6. The Council will facilitate all data subject rights under UK GDPR Articles 15 to 22, including subject access, rectification, erasure, restriction, objection, and rights in relation to automated decision-making and data portability.

9.7. Rights requests must be acknowledged promptly and responded to within one calendar month, extendable by two months for complex or numerous requests. Any extension or refusal must be reasoned and must inform the requestor of their right to complain.

9.8. For further guidance, contact the Information Governance Officer (see contact details on page 18 below).

Data protection complaints

9.9. The Council operates a published data protection complaints procedure in accordance with DPA 2018 §164A. A data protection complaint is any expression of dissatisfaction about how the Council has handled personal data; it does not need to reference legislation to qualify.

The Council will:

- acknowledge every complaint within 30 calendar days of receipt;
- investigate without undue delay and keep the complainant informed;
- communicate the outcome with reasons and advise the complainant of their right to escalate to the Information Commission; and
- log all complaints centrally with clear ownership, outcomes, and learning actions.

9.10. Complaints may be submitted in any form. Complaints received through any channel are valid and must be escalated to the DPO without delay. See contact details below.

9.11. Individuals who remain dissatisfied after receiving the Council's outcome may refer their complaint to the Information Commission (see contact details on page 14 under roles and responsibilities).

Freedom of Information and Environmental Information requests

9.12. The Council will meet its obligations under FOIA and the EIRs to respond to all valid requests within 20 working days, subject to applicable exemptions and exceptions. See contact details on page 18 below.

9.13. Requests will be handled without knowledge of the applicant’s identity or their purpose in seeking the information.

9.14. The Council will proactively publish disclosures and maintain its publication scheme in accordance with its publication scheme.

Information sharing

9.15. Personal data may only be shared with third parties where there are a lawful basis and a legitimate purpose. International transfers outside the UK require an adequacy decision, appropriate safeguards, or a recognised exception.

Confidentiality, security and potential data breaches

9.16. Officers and Members must not access, copy, alter, or disclose personal data except as authorised by their role and relevant legislation. The Council's ICT Security Policy applies to all electronic personal data.

9.17. A personal data breach is any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. On discovery of a potential breach, the reporting officer must notify the Corporate Governance team without delay via the incident form under 9.20 above. The Data Protection Officer or their nominated delegate will investigate the potential breach and assess severity.

9.18. Under UK GDPR Article 33, breaches likely to result in risk to individuals' rights and freedoms must be reported to the Information Commission within 72 hours. Under Article 34, where the risk is high, affected data subjects must also be notified directly.

9.19. All breaches will be logged and recommendations arising from investigations reported quarterly.

9.20. Suspected weaknesses or potential breaches must be reported without delay to the Corporate Governance team. Officers and elected Members should use the designated internal reporting eform. Members of the public should contact the Data Protection Officer or another Council officer who can pass the issue on (see contact details on page 18 below).

Information risk management and data protection impact assessments

9.21. Under UK GDPR Article 35, prior to commencing any processing likely to result in high risk to data subjects' rights and freedoms, a data protection impact assessment must be completed and reviewed by the Data Protection Officer.

9.22. Privacy by design must be embedded from the outset of any new project, system, or policy. Screening questions and templates are available to all officers. See **Appendix C: Data Protection Impact Assessments** for further information and guidance.

Article 30 records of processing activity and information asset registers

9.23. The Council maintains records of its processing activities as required by UK GDPR Article 30. Information Asset Owners are accountable for ensuring their respective Directorate's Article 30 records and information asset registers are accurate and current.

9.24. Records are operationally maintained by Information Governance Leads and reviewed in accordance with the timetable set by the Data Protection Officer.

Retention

9.25. Personal data is retained only for as long as necessary and in accordance with the Council's Data Retention Policy and accompanying data retention schedules.

9.26. The Council's privacy notices, published on its website, inform individuals of how their data is used and for how long.

9.27. See **section 15 Associated documents** for further information.

Contact details

9.28. The Data Protection Officer and Information Governance Officer can be reached using these contact details:

> Borough Council of King's Lynn and West Norfolk
> Kings Court, Chapel Street, King's Lynn PE30 1EX
>
> Telephone: **01553 616200**
>
> Email for freedom of information and environmental information requests:
> **freedom.information@west-norfolk.gov.uk**
>
> Email for all other information governance matters:
> **data.protection@west-norfolk.gov.uk**

10. Governance arrangements and oversight

Performance reporting

10.1. The Data Protection Officer (DPO) will compile an annual performance report on Information Governance and Data Protection to the Council's Corporate Performance Panel. This will be alongside regular updates to the Council's Executive Leadership Team.

Designation of key personnel

10.2. The DPO role will normally be fulfilled by a suitably qualified member of the paid service as part of a wider remit. It will be the task of the supervising Assistant Director or Executive Leadership Team member to designate the DPO clearly in the relevant job description and to confirm the appropriate seniority for the post through the Council's job evaluation process.

10.3. The Data Protection Officer will identify and designate a Deputy Data Protection Officer (DDPO) to provide cover for leave and routine absences. The DDPO will be suitably trained to act on behalf of the DPO, with a route of escalation to the Senior Information Risk Officer (SIRO) or their nominated deputy.

10.4. Should the DPO be unavailable for an extended period, the SIRO will determine what contingency arrangements fit the circumstances.

Policy review mechanism

10.5. This policy will be reviewed every two years, or at the time of legislative or major organisational change, whichever is sooner.

11. Additional information, guidance, and resources

Guidance from the Information Commission

The Information Commission is the independent regulator responsible for enforcing relevant legislation around people's data rights in the United Kingdom. It has broad investigatory and corrective powers.

Its website gives a broad range of guidance for both individuals and organisations, as well as details of how to escalate issues to the Commission.
ico.org.uk/for-the-public/

Information on the Council's website

The Council's web page on Data Protection gives information about our commitment and individuals' rights, as well as contact details and links to relevant request forms:
west-norfolk.gov.uk/info/20006/council_and_democracy/326/data_protection

The web page on Freedom of Information sets out our commitment to the legislative requirements, our publication scheme, how to seek an internal review of our response, and relevant contact details.
west-norfolk.gov.uk/info/20006/council_and_democracy/327/freedom_of_information

12. Health implications

12.1. No explicit health implications arise from this policy.

13. Environmental implications

13.1. No explicit environmental implications arise from this policy.

14. Equality, diversity and inclusion

14.1. The effects of this policy on protected characteristics defined in law, as well as further in the Council's policies, are neutral.

14.2. The small risk to equity of access to these provisions is mitigated through use of multiple channels (e.g. eforms, email, mail, phone, in-person appointments), plus use of translation services and supported guidance.

14.3. A pre-screening equalities impact assessment was included in the report submitting this policy to Cabinet (meeting date 9 June 2026 reference CAB12).

15. Associated documents

15.1. This policy is part of a suite of policies and procedures that should be used in conjunction with each other. Key linkages are with the following associated documents:

- Privacy Notice and associated departmental policies
  west-norfolk.gov.uk/privacy
- Data Retention and Disposal Policy and departmental schedules
  west-norfolk.gov.uk/downloads/download/820/data_retention_and_disposal_policies
- Freedom of Information Publication Scheme
  west-norfolk.gov.uk/downloads/download/617/freedom_of_information
- ICT Security Policy (internal)
- ICT Computer Usage Policy (internal)

Appendix A: The Personal Data Protection Principles

UK GDPR Article 5 requires us to abide by a set of six data protection principles:

A1. Lawfulness, fairness and transparency

Processing must have a valid lawful basis; must not deceive or harm the data subject; and individuals must be informed about how their data is used in clear, accessible terms.

> Example: A housing benefits team processes applicants' financial data under the lawful basis of legal obligation (Housing Benefit Regulations 2006). The service's privacy notice, published on the Council's website and available in the benefits office, sets out in plain English what data is collected, why, and how long it is kept.

A2. Purpose limitation

Data collected for one specified purpose must not be used for a different, incompatible purpose without a fresh lawful basis or the data subject's consent.

> Example: Contact details collected by the Council's leisure centre for membership administration must not be passed to the planning department to consult residents on a nearby development without separate authority to do so.

A3. Data minimisation

Only data that is adequate, relevant, and limited to what is necessary for the purpose should be collected and held.

> Example: An environmental health officer investigating a noise complaint needs the complainant's contact details and address, but not their date of birth, employment status, or other personal details that play no part in investigating the complaint.

A4. Accuracy

Personal data must be accurate and, where necessary, kept up to date. Inaccurate data must be corrected or erased without delay.

> Example: A resident notifies the Council that they have moved house. The Council tax, housing register, and any other relevant service records must be updated promptly. Holding an old address across multiple systems risks incorrect billing, missed correspondence, and potential enforcement action against the wrong person.

A5. Storage limitation

Personal data must not be kept in a form that identifies individuals for longer than is necessary for the purpose for which it was collected.

> Example: Planning application files contain personal data about applicants and objectors. Once an application is determined and any appeal period has elapsed, personal data that is no longer needed for legal or administrative purposes should be reviewed against the Council's Retention and Disposal Policy and disposed of securely, not retained indefinitely simply because storage is cheap.

A6. Integrity and confidentiality (security)

Personal data must be processed securely, with appropriate technical and organisational measures to protect against unauthorised or unlawful processing, and against accidental loss, destruction, or damage.

> Example: A licensing officer emailing a list of personal licence holders to an external contractor must use secure transfer methods and must not send unencrypted personal data to a personal email address. Physical files containing enforcement records must be stored in locked cabinets and not left unattended in open-plan areas or vehicles.

A7. Accountability

A seventh overarching obligation, accountability, requires the Council to be able to demonstrate compliance with all the above principles. This is addressed through this policy, the Council's Article 30 records, staff training, DPIAs, and governance reporting arrangements.

Appendix B: Processing personal data

B1. Lawful bases for processing personal data

The basis for processing personal data must be lawful. At least one of the following bases under UK GDPR Article 6 must apply whenever the Council processes personal data:

- **Consent:** the individual has given clear consent for the Council to process their personal data for a specific purpose. Consent can be withdrawn at any time.
- **Contract:** the processing is necessary for a contract the Council has with the individual, or because they have asked the Council to take specific steps before entering a contract.
- **Legal obligation:** the processing is necessary for the Council to comply with the law.
- **Vital interests:** the processing is necessary to protect the vital interests of the data subject or another person.
- **Public task:** the processing is necessary for the Council to perform a task in the public interest or for its official functions, and the task or function has a clear basis in law.
- **Legitimate interests:** note that this basis cannot be used for processing carried out by public authorities in the performance of their tasks.

B2. Appropriate policy document (DPA 2018 Schedule 1, Part 4)

The Data Protection Policy and this appendix to it serve as the Appropriate Policy Document (“APD”) for the purposes of Schedule 1, Part 4 of the Data Protection Act 2018. It is required where the Council processes special category data or criminal offence data under a Schedule 1 condition.

The Council's operational needs to process special category and criminal offence data are perpetual in nature. This Policy, including this Appendix, will be retained for as long as these processing activities continue and for a minimum of six months after any relevant processing activity permanently ceases. Superseded versions of this Policy will be retained for six months following replacement.

B3. Conditions for processing special category data

Special category ("SC") data is personal data that warrants extra protection by reason of its sensitivity. Under UK GDPR Article 9, SC data comprises personal data revealing:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data processed to uniquely identify a person
- data concerning health
- data concerning a person's sex life
- data concerning a person's sexual orientation

To process special category data, the Council must identify and document both a lawful basis under Article 6 (above) and a separate condition under Article 9. The conditions under Article 9 are:

- Explicit consent of the data subject
- Necessary for employment, social security or social protection law (requires an APD and, in most cases, an Appropriate Policy Document condition under Schedule 1 DPA 2018)
- Necessary to protect the vital interests of the data subject or another person where the data subject is physically or legally incapable of giving consent
- Processing by a not-for-profit body in the course of its legitimate activities, relating only to members or former members or persons with regular contact with the body
- Personal data manifestly made public by the data subject
- Necessary for the establishment, exercise or defence of legal claims
- Necessary for reasons of substantial public interest (requires an APD)
- Necessary for preventative or occupational medicine, medical diagnosis, health or social care, or management of health or social care systems (requires an APD)
- Necessary for public health purposes (requires an APD)
- Necessary for archiving in the public interest, scientific or historical research, or statistical purposes (requires an APD)

A DPIA must be completed and documented where the processing of special category data is likely to result in high risk to data subjects.

B4. Conditions for processing criminal offence data

Criminal offence ("CO") data is personal data relating to criminal convictions, offences, allegations, investigations, or proceedings, including unproven allegations, information relating to the absence of convictions, and data relating to victims and witnesses. It also covers related security measures: penalties, conditions or restrictions imposed as part of the criminal justice process, and civil measures which may lead to a criminal penalty.

To process criminal offence data, the Council must identify and document both a lawful basis under Article 6 and either official authority under Article 10, or a separate condition under Schedule 1 of the DPA 2018.

As a public authority, the Council must identify the specific statutory provision conferring official authority where it relies on that basis. Where official authority is not applicable, the relevant Schedule 1 condition must be identified. The Schedule 1 conditions most likely to be relevant to a district council include:

- Employment, social security, and social protection (para. 1)
- Health or social care purposes (para. 2)
- Public health (para. 3)
- Research (para. 4)
- Statutory and government purposes (para. 6)
- Administration of justice and parliamentary purposes (para. 7)
- Preventing or detecting unlawful acts (para. 10)
- Protecting the public against dishonesty (para. 11)
- Regulatory requirements relating to unlawful acts and dishonesty (para. 12)
- Preventing fraud (para. 14)
- Suspicion of terrorist financing or money laundering (para. 15)
- Safeguarding of children and individuals at risk (para. 18)
- Elected representatives responding to requests (para. 23)
- Disclosure to elected representatives (para. 24)
- Legal claims (para. 33)
- Insurance (para. 37)

A DPIA must be completed and documented where the processing of criminal offence data is likely to result in high risk to data subjects.

B5. How the Council secures compliance with the data protection principles when processing SC and CO data

Pursuant to Schedule 1, Part 4, paragraph 39(2)(a) of the DPA 2018, the Council applies the following measures when processing special category or criminal offence

data, in addition to its general compliance framework set out in this Policy and Appendix A:

a) **Governance and authorisation.** Processing of SC or CO data must be documented in the relevant Directorate's Article 30 record before it commences. The lawful basis, Article 9 condition or Schedule 1 condition, and (where required) the Appropriate Policy Document condition must all be identified and recorded. Where a new processing activity is proposed, this must be approved by the IAO for the relevant Directorate and reviewed by the DPO.

a) **Privacy by design and DPIAs.** Where proposed processing of SC or CO data is likely to result in high risk to data subjects' rights and freedoms: as is commonly the case given the sensitivity of these categories: a DPIA must be completed and signed off by the DPO before processing commences. See Appendix C.

b) **Access controls.** Access to SC and CO data is restricted to officers with a legitimate need to process it in the performance of their duties. Access rights are managed through the Council's ICT systems and reviewed periodically. Physical files containing SC or CO data are stored securely and accessible only to authorised staff.

c) **Staff training.** All officers are required to complete the mandatory data protection e-learning module, which covers the additional obligations applicable to SC and CO data. Officers in services that routinely process SC or CO data: including housing, environmental health, licensing, revenues and benefits, and HR: receive additional awareness as part of service induction and periodic briefing by IG Leads.

d) **Data sharing.** SC and CO data is shared with third parties only where there is a clear lawful basis, a legitimate purpose, and (where required) a written data sharing agreement or data processing agreement. Disclosures are made only to those with a legal entitlement to receive the data. Ad hoc disclosures outside agreed frameworks are not permitted.

e) **Minimisation and pseudonymisation.** The Council applies data minimisation to SC and CO data as a matter of course: only data that is necessary for the specific purpose is collected and retained. Where feasible, pseudonymisation or anonymisation techniques are applied, particularly in research, reporting, and analytical contexts.

f) **Breach response.** Breaches involving SC or CO data are treated as higher priority in the Council's breach assessment process, given the greater

potential for harm to data subjects. The DPO will consider whether Information Commission notification and direct subject notification are required on the facts of each breach.

B6. Retention of special category and criminal offence data

This section satisfies the requirement under Schedule 1, Part 4, paragraph 39(2)(b) DPA 2018.

Personal data, including special category and criminal offence data, is retained only for as long as is necessary for the purpose for which it was collected. The Council's departmental retention schedules, published on the Council's website, are the authoritative source for retention periods and must be consulted by officers and IG Leads in respect of specific record types.

The following sets out the Council's principal processing activities involving SC or CO data and the schedule in which the applicable retention periods are found.

Special category data

Processing activity	**Data types**	**Schedule and reference**
Housing options, homelessness assessment and prevention	Health and medical information, vulnerability and occupational support needs assessments, carer information, MARAC and MAPPA information	HWPP4.1.1 HWPP4.1.2
Housing standards enforcement, disrepair, harassment and illegal eviction, housing assistance and grants	Health and medical information	HWPP4.2.1 HWPP4.2.2 HWPP4.2.7
Unauthorised encampments	Health and medical information	HWPP4.2.5
Care and Repair: Disabled Facilities Grants and Handy Person Scheme	Health and medical information	HWPP2.1.1 HWPP2.1.2
Careline Community Alarm and associated services	Health and vulnerability data	HWPP3.1.1
Environmental health: accidents and injuries involving adults	Health data	HWPP6.5.1
Environmental health: accidents and injuries involving children	Health data	HWPP6.5.2

Processing activity	Data types	Schedule and reference
Benefits assessment, payment and fraud investigation	Medical forms, health and financial vulnerability data	R2.1.1 to R2.1.13
Personnel and payroll: all employees	Health and medical information, trade union membership, occupational health, DBS records, equality monitoring, safeguarding referrals	CS5.1 to CS5.13
Licensing: hackney carriage, private hire drivers and operators	Medical information, right to work	CE4.1.9 CE4.2.1 CE4.2.2
Standards: investigation of complaints about conduct of councillors	Personal appearance and behaviour, political affiliation and opinions, health information	CE3.10.1
Customer Information Centre data collection for housing, care, licensing and community safety services	Health and financial data	CS2.1.3 to CS2.1.8
Communications: photographs	Images of identifiable individuals	CS1.1.2

Criminal offence data

At the time of writing (April 2026), the Council's departmental retention schedules do not systematically distinguish criminal offence data as a distinct category. The schedules address records that contain CO data, including community safety, enforcement, prosecution, licensing and fraud investigation records. However, these are treated within a general framework that does not explicitly engage with the additional requirements applicable to CO data under UK GDPR Article 10 and Schedule 1 DPA 2018.

This is a known gap to be addressed as part of the planned review of the Data Retention Policy and departmental schedules. In the interim, the following schedule entries cover the record types most likely to contain CO data:

Processing activity	Data types	Schedule and reference
Community safety, ASB case management, waste enforcement, service of notices, prosecution of cases, injunctions and other ASB interventions	Criminal records, offence and conviction data, case evidence	HWPP1.1.1 to HWPP1.1.7
Unauthorised encampments	Criminal records	HWPP4.2.5

Processing activity	Data types	Schedule and reference
Health and safety enforcement notices	Offence and prosecution data	HWPP6.1.1
Benefits fraud investigation: no fraud established or no further action	Investigation records, interview records	R2.1.8 R2.1.9
Benefits fraud investigation: sanction applied (caution, administrative penalty or prosecution)	Conviction and sanction data, interview records	R2.1.10
Benefits fraud investigation: prosecution resulting in acquittal	Offence and acquittal data, evidence	R2.1.11
Benefits fraud: QB50 notebooks	Investigation notes	R2.1.12
Internal audit: investigation resulting in caution	Offence and caution data	R3.1.8
Internal audit: investigation resulting in administrative penalty	Penalty and offence data	R3.1.9
Internal audit: investigation resulting in prosecution	Conviction data	R3.1.10
Internal audit: RIPA surveillance records	Surveillance and intelligence data	R3.1.12
Licensing: hackney carriage, private hire drivers and operators (refusals, revocations and suspensions)	Criminal record data, conviction history	CE4.1.9 CE4.2.1 CE4.2.2
Licensing: licensing hearings generally	Convictions, criminal background data	CS4.3.8
RIPA authorisations: revenues and benefits	Surveillance records	R2.1.2
RIPA authorisations: legal	Surveillance records, observation logs, authorisations	CE3.5.1
Standards: investigation of complaints about conduct of councillors	Offences, alleged offences	CE3.10.1

General principles

Regardless of the specific period applicable to a record type, SC and CO data must be reviewed at the end of the applicable retention period and erased promptly unless a statutory obligation, legal proceedings, or a legitimate operational need requires continued retention. Erasure must be carried out securely in accordance with the Council's Data Retention Policy. IAOs are accountable for ensuring their Directorate's schedules adequately address SC and CO data as distinct categories and must treat any unresolved or outstanding schedule entries as an open compliance risk requiring prompt resolution.

Appendix C: Data Protection Impact Assessments

C1. Introduction

Under GDPR, there is an obligation for organisations, in their role as data controllers, to conduct a data protection impact assessment ("**DPIA**") before undertaking any processing that presents a specific privacy risk by virtue of its nature, scope or purpose.

Article 35 of GDPR introduces the formal requirement for a DPIA and it can best be described as a type of risk assessment which is carried out prior to a new processing activity, to highlight the viability of carrying out such a process and identifying any risks that may be associated with the processing.

C2. When is a DPIA required?

Article 35 sets out the circumstances where a DPIA is required and states:

> *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."*

Although GDPR does not specifically state what must be covered by a DPIA, Article 35(7) sets out the following minimum requirements that should be considered:

- A systematic description of the proposed processing operations
- The purposes of the processing
- The legitimate interest pursued by the controller
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- An assessment of the risks to the rights and freedoms of data subjects
- The measures envisaged to address the risks, including appropriate: safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance considering the rights and legitimate interests of data subjects and other persons concerned.

C3. When is a DPIA not required?

The GDPR doesn't specifically state when a DPIA is not required, but there is significant guidance which can be relied upon when deciding whether a DPIA is

required or not. From this guidance several circumstances have been identified where a DPIA is not required. These are:

- Where processing is low risk (i.e. not likely to result in a high risk to the rights and freedoms of natural persons).
- Where a DPIA has already been carried out and the nature, scope, context, and purposes of the processing are very similar to the proposed processing.
- Where a processing operation has a legal basis in EU or Member State law and has stated that an initial DPIA does not have to be carried out, where the law regulates the specific processing operation and where a DPIA, according to the standards of the GDPR, has already been carried out as part of the establishment of that legal basis.
- Where the processing is included on the optional list (established by the INFORMATION COMMISSION) of processing operations for which no DPIA is required

The Information Commission publishes a useful guide on Data Protection Impact Assessments on its website:
ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

Templates and screening questions to ascertain the need for a DPIA are published for staff on the Council's intranet. The screening questions are based on Information Commission guidance.

C4. Action Plan

These are a few points that you should consider when looking at DPIAs and whether you feel it is necessary to carry out an assessment:

- Be aware of the data you / your department processes and regularly assess whether this is due to change.
- If your department has been tasked with a new exercise, go through the screening questions on the template DPIA to determine whether you need to carry out the assessment.
- Look for any potential risk factors associated with the data you process and determine whether an assessment is needed.