The Arc
High Street
Clowne
S43 4JY

To: Chair & Members of the Customer Services Scrutiny Committee

Contact: Coby Bunyan
Telephone: 01246 242520
Email: coby.bunyan@bolsover.gov.uk

Monday 27th, April 2026

Dear Councillor,

EXTRAORDINARY CUSTOMER SERVICES SCRUTINY COMMITTEE

You are hereby summoned to attend a meeting of the Customer Services Scrutiny Committee of the Bolsover District Council to be held in the Council Chamber, The Arc, Clowne on Tuesday, 5th May, 2026 at 10:00 hours.

Register of Members' Interests - Members are reminded that a Member must within 28 days of becoming aware of any changes to their Disclosable Pecuniary Interests provide written notification to the Authority's Monitoring Officer.

You will find the contents of the agenda itemised on page 3 onwards.

Yours faithfully

J. S. Fieldend

Solicitor to the Council & Monitoring Officer

Equalities Statement

Bolsover District Council is committed to equalities as an employer and when delivering the services it provides to all sections of the community.

The Council believes that no person should be treated unfairly and is committed to eliminating all forms of discrimination, advancing equality and fostering good relations between all groups in society.

Access for All statement

You can request this document or information in another format such as large print or **language** or contact us by:

- **Phone:** 01246 242424
- **Email:** enquiries@bolsover.gov.uk
- **BSL Video Call:** A three-way video call with us and a BSL interpreter. It is free to call Bolsover District Council with Sign Solutions, you just need WiFi or mobile data to make the video call, or call into one of our Contact Centres.
- Call with Relay UK - a free phone service provided by BT for anyone who has difficulty hearing or speaking. It's a way to have a real-time conversation with us by text.
- **Visiting** one of our offices at Clowne, Bolsover, Shirebrook and South Normanton

EXTRAORDINARY CUSTOMER SERVICES SCRUTINY COMMITTEE
AGENDA

Tuesday, 5 May 2026 at 10:00 hours taking place in the Council Chamber, The Arc, Clowne

Item No.		Page No.(s)
1.	**Apologies For Absence** To receive apologies.	
2.	**Declarations of Interest** Members should declare the existence and nature of any Disclosable Pecuniary Interest and Non Statutory Interest as defined by the Members' Code of Conduct in respect of: a) any business on the agenda b) any matters arising out of those items and if appropriate, withdraw from the meeting at the relevant time.	
3.	**New Draft Data Protection Polices**	4 - 59

BOLSOVER DISTRICT COUNCIL

Meeting of the Customer Services Committee on 5th May 2026

2026 Data Protection Policy

Report of the Information & Engagement Manager

Classification	This report is Public
Contact Officer	Information & Engagement Manager

PURPOSE/SUMMARY OF REPORT

The purpose of this report is to provide the updated 2026 Data Protection Policy to the Customer Services Scrutiny Committee for consideration prior to being submitted to the Executive for approval.

The report seeks approval of the revised Data Protection Policy (Version 2.1), which has been updated to ensure continued full compliance with the UK GDPR (as amended), the Data Protection Act 2018, and the Data (Use and Access) Act 2025 (DUAA).

REPORT DETAILS

1. Background

1.1 Bolsover District Council takes the security and privacy of data seriously and is committed to being transparent about how we collect and use personal data and meet our data protection obligations. We are registered as a "data controller" with the Information Commissioner's Office (IC0) (registration number: Z670917X) and it is our duty to comply with our legal obligations under the Data Protection Act 2018 (the Legislation), the UK GDPR (as amended by the Data (Use and Access) Act 2025), and in consideration of other regulations, information security standards and other good practice standards.

1.2 The Data (Use and Access) Act 2025 received Royal Assent on 19 June 2025. Most of its data protection provisions came into force on 5 February 2026, with a further statutory right to complain directly to organisations taking effect on 19 June 2026. As a data controller, Bolsover District Council is required to keep its policies and practices up to date to reflect these legislative changes. This revision maintains the Council's strong accountability framework while incorporating the new lawful basis, improved flexibility on automated decision-making, updated international transfer rules, and enhanced protections for children's data.

2. Details of Proposal or Information

2.1 This Policy sets out the Council's commitment to data protection and individual rights in relation to personal data and sensitive personal data. It explains how the Council will hold and process personal information and explains individuals' rights as a "data subject".

2.2 This Policy applies to all employees, Councillors, contractors, apprentices, agency staff and unpaid volunteers and those on work experience. It covers personal data we collect and use on paper and electronically. It covers our corporate databases, network, video and photographs, voice recordings, CCTV, Body Worn Video (BWV) and mobile devices.

2.3 The policy has been refreshed with the following targeted, proportionate changes (all other sections remain unchanged and continue to reflect best practice):

2.4 New recognised legitimate interests lawful basis (Article 6(1)(ea) UK GDPR) – added as the seventh lawful basis. This removes the need for a separate balancing test for specific public-interest purposes listed in Annex 1 (e.g., prevention/detection of crime, safeguarding, emergencies, national security). Reliance on this basis will be recorded in the Register of Processing Activities.

2.5 Automated decision-making (ADM) – updated wording to reflect the greater flexibility introduced by the DUAA while retaining appropriate safeguards, human intervention rights, and restrictions on special category data.

2.6 International transfers – clarified use of the new statutory data protection test and Transfer Risk Assessment (TRA) process.

2.7 Privacy by Design / DPIAs – explicit requirement to give particular consideration to children's higher protection and age-appropriate design where relevant.

2.8 Individual rights – new section confirming the statutory right to complain directly to the Council from 19 June 2026. This is supported by the new Data Protection Complaints Procedure (now listed as a related document).

2.9 Privacy notices – commitment to regular review to reflect the new lawful basis and other DUAA changes.

2.10 Related policies/procedures – updated cover sheet and section 25 to include the new Data Protection Complaints Procedure and forthcoming Guidance on the DUAA amendments (June/July 2026).

2.11 The policy continues to meet all ICO accountability expectations and remains suitable for publication under the Freedom of Information Act 2000.

3. Reasons for Recommendation

3.1 The previous policy referenced outdated guidance and legislation. Without the proposed new policy, staff would continue to rely on inaccurate or inconsistent materials, thereby reducing confidence in the Council's policy framework and undermining its ability to demonstrate compliance with accountability

requirements. The proposed Data Protection Policy has been introduced to fully comply with up-to-date legal obligations.

3.2 The proposed Data Protection Policy outlines the levels of **accountability** for the Council's handling of personal information which includes:

- The Council's Chief Executive Officer who is accountable for providing the policies for employees to follow under the law to meet statutory requirements.
- The Council's Senior Information Risk Officer (SIRO) who is accountable for protecting the Council's information assets.
- The Council's DPO who is required in law to ensure the Council complies with data protection legislation.

4 Alternative Options and Reasons for Rejection

4.1 No alternative options are proposed as the policy is required to meet relevant regulations, legislation and guidance.

RECOMMENDATION(S)

1. That Members review the attached Data Protection Policy and provide comments for consideration as part of the development of the Policy in advance of formal Executive approval and implementation.

Approved by Councillor Donna Hales, Portfolio Holder for Corporate Performance and Governance

---

IMPLICATIONS:

Finance and Risk **Yes☐** **No ☒** **Details:** There are no direct financial implications arising from this report. On behalf of the Section 151 Officer
Legal (including Data Protection) **Yes☒** **No ☐** **Details:** The legal obligations are listed within the Policy. The Policy has been developed in line with the legal and regulatory requirements. Failure to discharge our responsibilities and obligations could result in compensation claims. Failure to comply with our duties under the DPA 2018 and the UK GDPR can potentially result in the ICO imposing substantial fines of up to £17.5 million, or 4% of the Council's annual turnover, whichever is higher. On behalf of the Solicitor to the Council

Staffing **Yes☐** **No ☒**
Details:

There are no staffing implications in the report arising from the proposed Data Protection Policy. Staff are aware of the updated (draft) Policy which was tabled at the Service Managers Forum. Additionally, staff have undertaken recent (updated) Data Protection training as part of the Council's online training solution (SkillGate) during September 2025.

On behalf of the Head of Paid Service

Equality and Diversity, and Consultation **Yes☐** **No ☒**
Details:

A consultation exercise was not required in devising the proposed Data Protection Policy which was compiled by the Council's Data Protection Officer (qualified GDPR Practitioner). An Equality Impact Assessment (EIA) was not required in devising the proposed Policy as no protected characteristic groups were identified as being impacted.

On behalf of Consultation & Equalities Lead

Environment **Yes☐** **No ☒**
Please identify (if applicable) how this proposal/report will help the Authority meet its carbon neutral target or enhance the environment.
Details:

N/A

DECISION INFORMATION:

☒ ***Please indicate which threshold applies:***	
Is the decision a Key Decision? A Key Decision is an Executive decision which has a significant impact on two or more wards in the District or which results in income or expenditure to the Council above the following thresholds:	**Yes☐** **No ☒**
Revenue (a) Results in the Council making Revenue Savings of £75,000 or more or **(b)** Results in the Council incurring Revenue Expenditure of £75,000 or more.	**(a)** ☐ **(b)** ☐
Capital (a) Results in the Council making Capital Income of £150,000 or more or **(b)** Results in the Council incurring Capital Expenditure of £150,000 or more.	**(a)** ☐ **(b)** ☐
District Wards Significantly Affected: *(to be significant in terms of its effects on communities living or working in an area comprising two or more wards in the District)* Please state below which wards are affected or tick **All** if all wards are affected:	**All** ☐

Is the decision subject to Call-In? (*Only Key Decisions are subject to Call-In*)	**Yes☐ No ☒**
If No/Yes, is the call-in period to be waived in respect of the decision(s) proposed within this report? ***(decisions may only be classified as exempt from call-in with the agreement of the Monitoring Officer)***	**Yes☐ No ☐**
Consultation carried out: *(this is any consultation carried out prior to the report being presented for approval)* **Leader ☐ Deputy Leader ☐ Executive ☐ SLT ☐** **Relevant Service Manager ☒ Members ☐ Public ☐** **Other ☐**	**Yes☐ No ☒**

Links to Council Ambition: Customers, Economy, Environment, Housing
Customers: Providing excellent and accessible services. The Council takes the security and privacy of data seriously for its staff and customers. We are responsible for managing the information we hold, and we recognise that this information is important to all staff and service users. We aim to use personal information fairly, correctly and safely in line with the legal requirements.

DOCUMENT INFORMATION:

Appendix No	Title
1	Old Data Protection Policy
2	Draft New Data Protection Policy
3	Draft Data Breach Management Policy
4	Draft Individual Rights Procedure
5	Draft Redaction Policy
6	Draft Data Protection Complaints Procedure

Background Papers
(These are unpublished works which have been relied on to a material extent when preparing the report. They must be listed in the section below. If the report is going to Executive, you must provide copies of the background papers).

Appendix 1

Data Protection Policy

July 2024

Equalities Statement

Bolsover District Council is committed to equalities as an employer and when delivering the services, it provides to all sections of the community.

The Council believes that no person should be treated unfairly and is committed to eliminating all forms of discrimination, advancing equality and fostering good relations between all groups in society.

Access for All statement

You can request this document or information in another format such as large print or **language** or contact us by:

- **Phone** - 01246 242424
- **Email** – enquiries@bolsover.gov.uk
- **BSL Video Call** – a three way video call with us and a BSL interpreter. It is free to call Bolsover District Council with Sign Solutions, you just need wifi or mobile data to make the video call, or call into one of our Contact Centres.
- Call with Relay UK via textphone or app on ***0800 500 888*** - a free phone service provided by BT for anyone who has difficulty hearing or speaking. It's a way to have a real time conversation with us by text.
- **Visiting** one of our offices at Clowne, Bolsover, Shirebrook and South Normanton

CONTROL SHEET FOR DATA PROTECTION POLICY

Policy Details	Comments / Confirmation (To be updated as the document progresses)
Policy title	Data Protection Policy
Current status – i.e. first draft, version 2 or final version	Final Version
Policy author (post title only)	Information, Engagement and Performance Manager
Location of policy (whilst in development)	S Drive
Relevant Cabinet Member (if applicable)	Portfolio holder for Corporate Governance
Equality Impact Assessment approval date	28/11/19
Partnership involvement (if applicable)	
Date policy approved	BDC DD/040/20/KD 25/06/20
Date policy due for review (maximum three years)	**2027** Reviewed July 2024
Date policy published	Reviewed version July 2024 Originally 01/07/20

DATA PROTECTION POLICY

1. Introduction

1.1. The processing of personal data is essential to many of the services and functions carried out by local authorities. Bolsover District Council ('the Council') recognises that compliance with data protection legislation will ensure that processing is carried out fairly and lawfully.

1.2. The Data Protection Act 2018 (DPA) is an Act of Parliament which updates data protection laws in the UK. It is national law which complements the UK General Data Protection Regulation (UK GDPR 2018, applicable 2021). The latter together form the framework for data protection law in the UK.

1.3. The Information Commissioner's Office (ICO) is the relevant supervisory authority for the UK. Set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

2. Scope

2.1 The policy is applicable to all employees, Elected Members, apprentices, agency workers, unpaid volunteers and those on work experience. In certain circumstances it will apply to contractors working for the Council.

2.2 This policy applies to the collection and processing of all personal data as defined by the legislation as that of a 'natural person'. It covers all formats including paper, electronic, audio and visual formats. The policy will only deal with the personal data of a living person and does not apply to the data of a deceased person.

2.3 The policy applies to all employees working within Elections although the post of Electoral Registration Officer is registered, for the processing of elections data, with the Information Commissioner's Office separately.

2.4 Organisations who process data on our behalf, will have their own policy statements in respect to data protection.

3. Principles

3.1 The policy sets out the main requirements of the data protection legislation and how the Council will comply. It is not a statement of how compliance will be achieved as this will be a matter for operational procedures and processes.

3.2 The policy will be made available to the public.

4. Data Protection Statement

4.1 Key Definitions (UK GDPR)

4.1.1 The UK GDPR applies to the processing of personal data that is wholly or partly by automated means or to the processing other than by automated means which forms part of, or is intended to form part of, a filing system. '**Filing system**' means any structured set of personal data, whether centralised, decentralised or dispersed on a functional or geographical basis.

4.1.2 '**Personal data'** means 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, a number, location data etc. This may also include online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers. Such identifiers may leave traces which combined with other information may be used to create profiles of the natural person and identify them.

4.1.3 The Council is the **'Data Controller'** who determines the purposes and means of processing personal data. **Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4.1.4 UK GDPR also applies to **'Data Processors'** who act on the controller's behalf and places further obligations on both parties. The 'Processor' means a natural or legal person, public body, agency or other body which processes personal data on behalf of the Council.

4.2. Data Protection Principles

4.2.1. The following **principles** relate to the processing of personal data and set out the main responsibilities for the Council under UK GDPR. Article 5 requires that personal data shall be:

(a) Processed lawfully, fairly and in a transparent manner in relation to the data subject. **(Lawfulness, fairness and transparency).**

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered incompatible with the initial purposes. **(Purpose limitation)**.

(c) Adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. **(Data minimisation).**

(d) Accurate and where necessary, kept up-to-date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay**. (Accuracy)**.

(e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this legislation in order to safeguard the rights and freedoms of the data subject. **(Storage limitation)**.

(f) 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. **(Security).**

4.3. Lawful Basis for Processing

4.3.1 The lawful bases for processing are set out in Article 6 of the UK GDPR. At least one of these must apply whenever the Council processes personal data:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply to public authorities processing data to perform their official tasks.)

4.4 Special Category Data

4.4.1 Special category data is broadly similar to the concept of sensitive personal data under the 1998 Data Protection Act and covers information about an individual's:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

4.4.2 To process sensitive data the Council must also satisfy a specific condition for processing under Article 9 of the UK GDPR.

4.4.3 This type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination. As such the Council must ensure that adequate organisational and technical measures are in place to safeguard this data.

4.4.4 The UK GDPR rules for sensitive (special category) data do not apply to information about criminal allegations, proceedings, or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures, set out in Article 10.

4.4.5 To process personal data about criminal convictions or offences, the Council must have both a lawful basis under Article 6 and either legal authority or official authority for the processing under Article 10.

4.4.6 Article 10 states that processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority. This means that the Council must either process the data in an official capacity or meet a specific condition in Schedule 1 of the Data Protection Act 2018 and comply with the additional safeguards set out in that Act.

4.5 Data Subject Rights

4.5.1 The UK GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object

- Rights in relation to automated decision making and profiling.

  The exercise of some of the rights is conditional upon the lawful basis for processing the personal data.

4.5.2 The Council will ensure that information on how to exercise these rights is made easily available to individuals through its staff, website, and appropriate documentation e.g., application forms.

4.5.3 Upon receipt of a verified request the Council has one month to respond and cannot charge a fee to deal with a request under most circumstances.

4.5.4 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

4.5.5 The Council must provide individuals with information including: purposes for processing personal data, retention periods for that personal data, and who it will be shared with. This is commonly referred to as 'privacy information'.

4.5.6 Articles 13 and 14 of the UK GDPR specify what information individuals have the right to be informed about. This information needs to be provided at the time the personal information is collected and must use clear and plain language. The information must be concise, transparent and easily accessible.

4.5.7 The Council will provide privacy information in a variety of ways including published privacy statements, privacy notices on forms and posters and through its staff.

4.5.8 Individuals have the right to obtain the following from the Council:

- confirmation that we are processing their personal data;
- a copy of their personal data; and
- other supplementary information – (this largely corresponds to the information that should be provided in a privacy notice).

This is commonly referred to as subject access.

4.5.9 An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them, or they are acting on behalf of someone).

4.5.10 Responding to a subject access request may involve providing information that relates both to the individual making the request and to another individual. The DPA 2018 says that we do not have to comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In these circumstances the Council will need to decide whether it is appropriate to do so in each case. This decision will involve balancing the data subject's right of access against the other individual's rights.

4.5.11 The Council may seek to confirm the identity of an individual before responding to a request if needed.

4.5.12 The Council will have in place operational processes for identifying and processing requests in line with legal requirements.

4.5.13 In some circumstances, the DPA 2018 provides an exemption from particular UK GDPR provisions. If an exemption applies, the Council may not have to comply with all the usual rights and obligations e.g., the right to be informed. The full list of exemptions are contained within Schedules 2-4 of the DPA 2018. Those covering crime and taxation and disclosures required by law or in connection with legal proceedings are the ones most likely to be relied upon by the Council. The Council considers the use of exemptions on a case-by-case basis and keeps records of its decisions.

4.5.14 Should any member of the public wish to make a complaint about the processing of their data by either of the Council then they should use the Council Complaints Procedure which is available on the website. The public also have a right to contact the Information Commissioners Office who are the supervisory authority for data protection matters under the legislation.

4.6 Accountability and Governance

4.6.1 Accountability is one of the data protection principles - it makes organisations responsible for complying with the UK GDPR and says that they must be able to demonstrate their compliance.

4.6.2 The Council will put in place appropriate technical and organisational measures to meet the requirements of accountability including:

- adopting and implementing data protection policies;
- putting written contracts in place with organisations that process personal data on our behalf;
- maintaining documentation of our processing activities;
- implementing appropriate security measures;
- recording and, where necessary, reporting personal data breaches;
- carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests and implement measures to meet the 'data protection by design and default' approach;
- appointing a data protection officer at an appropriate level within the organisation and provide suitable resources to support the role.

4.6.3 Accountability obligations are ongoing. The Council will keep its measures under review and update, where necessary.

4.7 Contracts

4.7.1 The UK GDPR makes written contracts between controllers and processors a requirement. (Rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the Data Protection Act 1998).

4.7.2 Contracts must include specific minimum terms. These terms are designed to ensure that processing carried out by a processor meets all the UK GDPR requirements, not just those related to keeping personal data secure.

4.7.3 The Council will only use processors that can give sufficient guarantees they will implement appropriate technical and organisational measures to ensure their processing will meet UK GDPR requirements and protect data subjects' rights.

4.8 Security

4.8.1 The Council is required to process personal data securely. This is not a new data protection obligation. It replaces and mirrors the previous requirement to have 'appropriate technical and organisational measures' under the Data Protection Act 1998.

4.8.2 The Council fully understands that poor information security leaves systems and services at risk and may cause real harm and distress to individuals. The Council takes their security obligations seriously.

4.8.3 The Council recognises that information security is important, not only because it is itself a legal requirement, but also because it can support good data governance and help us demonstrate our compliance with other aspects of the UK GDPR.

4.8.4 The Council will have technical and organisational measures in place to ensure a level of security appropriate to the risk of the personal data processing. These security measures will seek to ensure that:

- the data can be accessed, altered, disclosed or deleted only by those we have authorised to do so (and that those people only act within the scope of the authority we give them);
- the data we hold is accurate and complete in relation to why we are processing it; and
- the data remains accessible and usable, i.e., if personal data is accidentally lost, altered, or destroyed, we should be able to recover it and therefore prevent any damage or distress to the individuals concerned.

4.8.5 The Council's technical measures will include physical and Information Technology (IT) security such as premises security, access control within the building including visitors, paper, and electronic waste, keeping IT equipment, especially mobile devices, secure, and cybersecurity e.g., network and information systems, data, online and device security.

4.8.6 The Council's organisational measures will include this policy, its Information Security policy and internal guidance, provision of advice and a point of contact via the Data Protection Officer, developing a cultural awareness around information security, periodic checks to ensure that security measures remain appropriate and training.

4.8.7 All employees will receive initial and refresher data protection training appropriate to the personal data processing activities they undertake. The training will be mandatory for new employees and take place during their induction. Thereafter all staff who process personal data will be required to undertake refresher training every two years. Information security training is a requirement for every new starter using IT equipment and usually undertaken on the first day of work. Thereafter all staff who use IT equipment will undertake refresher training every two years. Elected Members will receive training on data protection and information security during their induction and thereafter as required.

4.9 Personal Data Breaches

4.9.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.

4.9.2 Under UK GDPR (Recital 87) when a security incident takes place, we need to quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including notifying the Information Commissioner's Office (ICO) if required.

4.9.3 The duty requires the Council to report certain types of personal data breach to the relevant supervisory authority (ICO) within 72 hours of becoming aware of the breach, where feasible.

4.9.4 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, then the Council must also inform those individuals without undue delay.

4.9.5 When notifying individuals, the Council will use clear and plain language to describe the personal data breach, provide contact details where more information can be obtained, describe any likely consequences of the personal data breach and the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

4.9.6 The Council must also keep a record of any personal data breaches, regardless of whether we are required to notify the ICO. The Council will document the facts relating to the breach, its effects and the remedial action taken.

4.9.7 The Council will investigate whether the breach was a result of human error or a systemic issue and consider how a recurrence can be prevented –

whether this is through better processes, further training or other corrective steps.

4.9.8 The Council will ensure that they have robust breach detection, investigation, and internal reporting procedures in place. A risk based approach will be used to facilitate decision-making about whether or not we need to notify the relevant supervisory authority (ICO) and the affected individuals.

4.10 International Transfers

4.10.1 The UK GDPR restricts the transfer of personal data to countries outside the European Economic Area (as individuals risk losing the protection of the UK GDPR).

4.10.2 A transfer of personal data outside the protection of the UK GDPR (referred to by the ICO as a 'restricted transfer'), most often involves a transfer from inside the EEA to a country outside the EEA.

4.10.3 Personal data which the Council process themselves is held on UK servers. When using an external provider for processing e.g., storing customer records, the Council will use companies which have UK/EU/EEA based servers or ensure that any restricted transfer is undertaken in accordance with UK GDPR provisions.

5. Responsibility for Implementation

5.1 Keeping the policy under review and updating the policy is the responsibility of the Data Protection Officer for the Council. The Senior Leadership Team are responsible for implementing this policy and the legislation in general.

5.2 Managers at all levels are responsible for ensuring that employees, agency workers, apprentices, unpaid volunteers and work placements for whom they are responsible are aware of and adhere to this policy. Managers are also responsible for ensuring that employees are updated in regard to any changes in this policy and receive regular training.

5.3 The Data Protection Officer assists the Council to monitor internal compliance, informs and advises on data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the supervisory authority (ICO).

Appendix 2

Data Protection Policy

2026

Cover sheet

Policy Title: Data Protection Policy

Related Policies/Procedures:

Data Breach Management Policy	Data Protection Complaints Procedure
Redaction Policy	Guidance on the Data (Use and Access) Act 2025 amendments (June/July 2026)

Contact: Information & Engagement Team (GDPR@bolsover.gov.uk)

Freedom of Information: This Policy is suitable for release under the Freedom of Information Act 2000.

Equality Impact Assessment: This Policy has been assessed as having no impact on any protected group.

Last reviewed: April 2026 (updated to reflect the Data (Use and Access) Act 2025)

Version: 2.1

Status: Not published

Comments: This policy has been updated to ensure continued compliance with the UK GDPR (as amended by the Data (Use and Access) Act 2025), the Data Protection Act 2018, and all other relevant legislation.

Contents

1. Summary

This policy sets out how the Council will comply with data protection legislation and protect the personal information of everyone who receives services from, or provides services to, the Council. It informs customers of their rights, and suppliers of their responsibilities. It shows how we comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, other regulations, information security standards and other good practice standards. The policy also reflects amendments introduced by the Data (Use and Access) Act 2025, which came into force on 5 February 2026.

2. Scope

This policy applies to all employees, Councillors, contractors, apprentices, agency staff and unpaid volunteers/those on work experience. It covers personal data we collect and use on paper and electronically. It covers our corporate databases, network and paper records. It covers video and photographs, voice recordings, CCTV, Body Worn Video (BWV) and mobile devices such as laptops, mobile phones and memory sticks. This policy also applies to all employees working within Elections although the post of Electoral Registration Officer is registered for the processing of elections data with the Information Commissioner's Office separately.

3. Accountability

Bolsover District Council is a data controller which means that it decides why and how personal data is processed. It is accountable for its handling of personal information.

Our *Chief Executive* is the person accountable for providing the policies for employees to follow under the law, so that we can carry out decisions of the Council in response to our statutory functions. The Data Protection Policy is part of our corporate information framework.

The *Senior Information Risk Officer* (SIRO) is the Director of Legal and Governance Services (Monitoring Officer) who is accountable for protecting the Council's information assets.

The *Data Protection Officer* is a position required in law to ensure the Council complies with data protection legislation.

Each *employee* and all *suppliers* are bound by a contractual duty of confidentiality.

The Council is registered with the *Information Commissioner's Office*, who is the independent regulator appointed by parliament to ensure compliance with data protection law.

The Council maintains a *Register of Processing Activities (ROPA)* otherwise known as an Information Asset Register of the personal information we are responsible for to ensure it is used according to the data protection principles.

All *Service Managers* are *Information Asset Owners (IAOs)* for the data processed by their service. They have responsibility for, and are held accountable for, the management of their Information Assets.

4. Definitions

The *UK General Data Protection Regulation* (UK GDPR) is the retained UK version of the General Data Protection Regulation (EU) 2016/679.

The *Data Protection Act 2018* is UK law which supplements UK GDPR

Personal information means any information relating to an identifiable **living** person. This means they can be identified from information such as a name, an address, an identification number (e.g. National Insurance number, NHS number or case reference number), location data, etc.

Special category data is data regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data and biometric data (fingerprints, eye scans etc.), data concerning health or data concerning a person's sex life or sexual orientation. There are extra safeguards for special category data to ensure no one is discriminated against when it comes to receiving a service.

The *processing* of data means any operation performed on personal data, whether using a computer or manual filing system. It includes collection, use, and recording, storing, sending and deleting personal data.

Information Governance (IG) is the control of information, assessing its value, ensuring it is appropriately managed, accessible, accurate, processed lawfully, secure and disposed of when appropriate.

Many organisations use the *Government Security Classification Scheme* marking all documents as Official, Sensitive etc. The Council requires marking of documents and considers all information to be confidential and decisions regarding publication, sharing of data etc. are made on this basis, i.e. all data must be held securely unless a legitimate decision to share has been reached.

5. Data Protection and Human Rights

Under the Human Rights Act 1998, everyone has the right to respect for their private and family life, their home and their correspondence. This includes respect for your private and confidential information, particularly when storing and sharing data.

This right can be limited in certain circumstances, but any limitation must balance the competing interests of an individual and of the community.

Any limitation must be covered by law and be necessary and proportionate for one or more of the following aims:

- public safety or the country's economic wellbeing
- prevention of disorder or crime
- protecting health or morals
- protecting other people's rights and freedoms
- national security.

The right to privacy must often be balanced against the right to free expression. Public figures do not necessarily enjoy the same privacy as others. For example, in some cases the public interest might justify publishing information about senior officers or Councillors even if it would otherwise interfere with their right to privacy.

6. Data Protection Principles

The Council is required to comply with the data protection principles when processing personal data. These principles are set out in the UK GDPR and have been incorporated into the Data Protection Act 2018. The six principles state that personal data must be:

- Processed lawfully, fairly and in a transparent way
- Collected for a specific purpose
- Adequate, relevant and limited to what's necessary
- Kept up to date and data is accurate
- Kept for only as long as necessary
- Protected with appropriate security.

7. Lawful Basis for Processing Personal Data

There are different lawful reasons for processing personal data and special category data. The Council must have at least **one** lawful basis for processing *personal information* and at least **one** lawful basis for processing *special category data*.

The seven lawful bases for processing personal data are:

1. The data subject has given clear consent to the processing of his or her personal data for one or more specific purposes

2. Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract

3. Processing is necessary for compliance with a legal obligation to which the controller is subject

4. Processing is necessary to protect the vital interests of the data subject or of another natural person

5. 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. 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, particularly where the data subject is a child.

7. Processing is necessary for the purposes of a recognised legitimate interest pursued by the controller or by a third party (new lawful basis introduced by the Data (Use and Access) Act 2025 and set out in Article 6(1)(ea) UK GDPR). This basis does not require a separate balancing test against the rights and freedoms of the data subject. It applies only to the specific public-interest purposes listed in Annex 1 to the UK GDPR, for example: prevention or detection of crime, safeguarding vulnerable individuals, responding to emergencies, national security, or disclosing data to public authorities exercising their public tasks.

The Council will document its reliance on any recognised legitimate interest in the Register of Processing Activities (RoPA).

Processing of **special category data** is prohibited unless one of the legal reasons in the list below apply:

1. The data subject has given explicit consent to the processing of their personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to above may not be lifted by the data subject.

2. Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment, social security or social protection law as authorised by domestic law, and subject to appropriate safeguards for the fundamental rights and the interests of the data subject.

3. Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

4. Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects.

5. Processing relates to personal data which are manifestly made public by the data subject.

6. Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

7. Processing is necessary for reasons of substantial public interest, based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

8. Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services based on domestic law or pursuant to contract with a health professional and subject to certain conditions and safeguards.

9. Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

10. Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) (as supplemented by section 19 of the 2018 Act) based on domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The Council must always demonstrate it processes information with safeguards in place to protect the fundamental rights and interests of the individual.

As the Council provides statutory services, we do not often rely on consent as the lawful basis (of those listed above) to process data. However, where we do, we must ensure that consent is freely given, it is not a precondition of a service, a record is kept of consent, and people can withdraw consent.

8. Duty of Confidentiality

Data processed by the Council is also subject to the common law duty of confidentiality. This means that information that has been given to a member of staff or a Councillor by an individual should not be used or disclosed further, except as originally understood by that individual, with their permission or where certain statutory functions need to be met. Please note that the duty of confidentiality continues after a person is deceased even when the data protection legislation would no longer apply.

Our staff and Councillors are subject to a Code of Conduct relating to confidentiality.

9. Information about Criminal Offences

The processing of information about criminal allegations, convictions or offences by the Council is in accordance with our legal obligations and because we have legal authority in certain areas such as preventing fly-tipping or upholding food hygiene and licensing of pubs and clubs.

10. Surveillance

The Council operates CCTV public safety. Body Worn Video (BWV) cameras are also used for a variety of purposes and are an effective way of reducing crime and protecting public safety. We operate under a Code of Practice prescribed by the Information Commissioner's Office (ICO).

The Council uses the Regulation of Investigatory Powers Act 2000 (RIPA) to conduct covert surveillance involving directed surveillance or the use of a covert human intelligence source (CHIS). The Council complies with the Codes of Practice that are overseen by the Investigatory Powers Commissioner's Office (IPCO). This is only for matters that the Council has responsibility for, and for directed surveillance must either involve a criminal offence which we are trying to prevent or detect, which is punishable by a maximum of at least 6 months imprisonment or would constitute an offence involving sale of tobacco and alcohol to underage children. The surveillance must be authorised by a magistrate.

The Council's Standards Committee receives a yearly report and monitors the use of such powers. We are also inspected by the IPCO.

11. Recording of Meetings

The Data Protection Act does not prevent members of the public recording meetings or conversations with a member of staff within a private meeting area or their home (including meeting rooms at Council premises). A member of the public is not a data controller for the purposes of the Act if they only use the recording for their own domestic purposes. For example, they may want to record a meeting to remind them what has been said, so they don't need to take notes and can fully engage in the meeting etc. Although this can feel intrusive, it is not a breach of staff's right to privacy as only professional matters will be discussed. However, if the recording is then published or used for other purposes, this processing may fall within the remit of the Data Protection Act.

If a member of the public wants to record a meeting, they should be advised that they can only do so for their own personal use and cannot publish the information or make it available via social media. If they ignore this advice, they should be asked to remove the information from the website/social media site. If they don't remove it, representation can be made to the provider to remove the content. Seek advice from the Council's legal services in such cases. If a member of staff records a meeting or conversation, this will be covered by the Act as it is made for professional purposes.

Members of the public cannot record, film or take photographs in open areas of our public buildings as we have a duty of care to customers accessing services. We offer a wide range of services in many Council buildings which means we may have vulnerable customers visiting us, including those with mental health conditions and customers fleeing domestic abuse. Therefore, it is vitally important that we provide a safe and secure place for them while they receive our help and support.

In a public building our customers should feel confident that they can enter and access services without being subject to recording or photographs.

For guidance about filming or taking photographs at a public Council meeting, please ask the Governance Team for their protocol.

12. Automated Processing

The Council may use automated decision-making (ADM), including solely automated decision-making that produces legal or similarly significant effects on individuals, where permitted under the UK GDPR (as amended by the Data (Use and Access) Act 2025). The amended rules provide greater flexibility for ADM while maintaining appropriate safeguards, particularly where special category data is involved. Where the Council relies on ADM that produces legal or similarly significant effects, we will:

• inform the individual

• provide simple ways for them to request human intervention, express their point of view, or contest the decision

• carry out regular checks to ensure our systems are working as intended; and

• apply appropriate safeguards, including technical and organisational measures to protect rights and freedoms.

The Council will not use solely automated decision-making based on special category data unless one of the Article 9 conditions and explicit safeguards apply.

13. Privacy Notices

The Council provides privacy notices, which are statements to individuals about how we will use their personal data. The information includes our purposes for processing their personal data, retention periods for that personal data, and who it will be shared with. This information can be found on the Council's website, and individuals are referred to it at the time we collect their personal data from them. Where we obtain personal data from other sources, we provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month. Privacy notices will be kept under regular review and updated to reflect the new recognised lawful basis (legitimate interests) and any other amendments introduced by the Data (Use and Access) Act 2025.

14. Individual Rights

Individuals whose data is processed by the Council have several rights in law. These are set out in the *Individual Rights Procedure*.

When a staff member/Council employee submits a Subject Access Request (SAR), the Council's HR service will administer this (retrieve, redact and disclose the necessary information) within one calendar month.

When a member of the public submits a SAR, the Council's Information & Engagement team will administer this (retrieve, redact and disclose the necessary information) within one calendar month.

The Council will disclose the requested information electronically as a matter of course unless otherwise agreed with the requestor, who may only be able to access the information by post.

From 19 June 2026, individuals will also have a new statutory right to complain directly to the Council about how their personal data has been processed. The Council will maintain a clear, accessible complaints process (including an electronic complaints form where practicable), acknowledge complaints within 30 days, and investigate without undue delay. Full details will be published on the Council's website and incorporated into the Individual Rights Procedure.

15. Information Sharing

The Council believes that the duty to share information can be as important as the duty to protect information. We have Information Sharing Agreements setting out the principles of information sharing with partners, such as DCC, NEDDC, the police, Department of Work and Pensions, etc. and these set out what data is being shared, how it is transferred and for what purpose it is shared.

16. Transfers of Data Outside the UK

Most of our processing occurs in the UK or countries covered by UK adequacy decisions. When personal data is transferred to third countries or international organisations, the Council will ensure the transfer is lawful under Chapter V of the UK GDPR (as amended).

We will apply the statutory data protection test (as updated by the Data (Use and Access) Act 2025) and complete a Transfer Risk Assessment (TRA) where required. Transfers will only proceed where an adequacy decision is in place, appropriate safeguards (such as the UK International Data Transfer Agreement or binding corporate rules) are implemented, or a relevant exception applies. The Council maintains records of all international transfers in line with our accountability obligations.

17. Privacy by Design / Data Protection Impact Assessments

The Council is committed to a privacy by design approach to building new systems and updating procedures for processing personal data. This means that we consider the risks to individual's privacy prior to the introduction of a new system or process. We use Data Protection Impact Assessments (DPIAs) to assess this risk when we introduce new technology or changes to the processing of personal data. The assessment identifies the risk to privacy from the customer's perspective and what steps can be taken to reduce this wherever possible whilst providing a service to the customer. Services introducing

new processing are responsible for ensuring that a DPIA is completed and is sent to the GDPR Team at GDPR@bolsover.gov.uk.

When conducting Privacy by Design activities or DPIAs, the Council will give particular consideration to children's higher protection matters (as required by the Data (Use and Access) Act 2025) where services are likely to be used by children. This includes assessing age-appropriate design and ensuring children's rights and freedoms are prioritised.

18. Contracts

Where the Council has a contractual relationship with another organisation or individual, we will ensure we are clear about the contractor's role, responsibilities and accountability in relation to personal information.

19. Information Security

The Council has both technical and operational measures in place to ensure that information is held and used securely. Guidance on how to use ICT equipment and what is considered as acceptable use is shared during staff induction and is also available by emailing the Service Desk.

Access to Information: All users with access to our data are authenticated and provided with a unique user ID. Access to information and systems will be based on access required for each individual role. Service areas will provide justification for the access requirements and management will authorise. Access to a system only authorises you to access records required for work purposes. You are not entitled to 'browse' records or look at files not relevant to your work.

Email: The Council's email system uses a security protocol that encrypts email for privacy which prevents unauthorised access of email when it's in transit over internet connections and by default, our email security system always tries to use a secure connection when sending email. The Council's standard retention policy for emails in Microsoft 365 is two years, after which emails are automatically deleted in line with our data minimisation obligations under Article 5(1)(e) UK GDPR.

Clear desk procedure: The Council operates a clear desk procedure. All information must be securely stored at the end of the working day and must not be accessible by anyone not authorised to access it. Filing cabinets are kept securely with restricted access.

Locking screens: When leaving their desks, staff must ensure they lock their screen so that information cannot be accessed inappropriately. Staff are aware of pressing 'windows key+L' to lock their screen as and when necessary, including when working at home so that family members or visitors cannot see their screen.

When working anywhere out of the office, staff must ensure their screen cannot be seen by other people.

Handling paper documents: Paper documents containing sensitive information must only be seen by authorised individuals. Keep these documents secure by storing them in fixed or portable lockers. When taking paper documents off-site ensure they are in your direct possession or line of sight, ideally in a locked case. Only take the minimum necessary to complete your business purpose. Ideally staff should scan documents such as registers, etc. and once safely saved on the restricted drive, they should shred or confidentially dispose of paper documents.

Malevolent Emails/Phishing: Email is an essential business tool. However, it is equally useful for criminals to gain unauthorised access to Council systems, information and passwords. Be especially vigilant for emails not addressed to you specifically, containing links navigating you to another website, or having attachments that you don't recognise. If you are suspicious of an email or mistakenly click on a link, it is essential you log this with the Service Desk straightaway.

Passwords: Contact ICT to provide guidance on setting a strong password if required.

Storing Electronic Information: Electronic information must only be stored on the Council network or on systems previously authorised by ICT.

Retention and Disposal: Information should be kept no longer than necessary in accordance with statutory or best practice retention periods. When information has reached the end of its retention period it should be disposed of in accordance with the Council's Retention & Disposal Schedule.

20. Data Protection Breaches

The Council tries hard to prevent information breaches, but when these occur, there is an incident reporting and investigation procedure. Where a breach is a risk to the rights and freedoms of anyone, it will be reported to the Information Commissioner's Office within 72 hours.

When information is accessed or disclosed inappropriately or any equipment or information is lost, the incident must be reported to GDPR@bolsover.gov.uk and the ServiceDesk.

Further information on how to report an incident/breach can be found in the Council's Data Breach Management policy.

The Information & Engagement team and ICT will investigate and take appropriate mitigation measures.

21. Human Resources

New members of staff and Councillors must complete the online data protection training when they receive their ICT equipment. All staff must complete the training every two years. It is the responsibility of managers to ensure this happens and that staff have adequate understanding of their data protection responsibilities.

All employee contracts make it clear that a breach of policy can lead to disciplinary action. Where staff have access to sensitive data additional safeguards may be implemented to provide a higher level of security, e.g. DBS checks for staff working directly with vulnerable adults or children.

22. Data Protection Officer

The Council has appointed a Data Protection Officer as required by law. Their role is to ensure the compliance of the Council with data protection law. The Data Protection Officer can be contacted by emailing GDPR@bolsover.gov.uk.

23. Compliance

Compliance with this policy is monitored by the Senior Information Risk Officer (SIRO).

24. References

●Data (Use and Access) Act 2025: https://www.legislation.gov.uk/ukpga/2025/18/contents
●UK GDPR is the retained EU law version of the General Data Protection Regulation (EU) 2016/679
●Data Protection Act 2018: https://www.legislation.gov.uk/ukpga/2018/12/contents
●Information Commissioner's Office: www.ico.org.uk

25. Related Policies and Procedures

This Data Protection Policy should be read with:

✓Bolsover District Council's guidance on the Data (Use and Access) Act 2025 amendments (to be published following full implementation – June/July 2026)
✓Data Breach Management Policy
✓Redaction Policy
✓Data Protection Complaints Procedure

Equalities Statement
Bolsover District Council is committed to equalities as an employer and when delivering the services, it provides to all sections of the community. The Council believes that no person should be treated unfairly and is committed to eliminating all forms of discrimination, advancing equality and fostering good relations between all groups in society.

Access for All statement
You can request this document or information in another format such as large print or language or contact us by:
Phone: 01246 242424
Email: enquiries@bolsover.gov.uk
BSL Video Call: A three-way video call with us and a BSL interpreter. It is free to call the Council with Sign Solutions or call into one of our Contact Centres.
Call with Relay UK via textphone or app on *0800 500 888* - a free phone service
Visiting one of our offices at Clowne, Bolsover, Shirebrook and South Normanton

Draft
Data Breach Management Policy
2026

Table of Contents

1. Purpose of this document

This document sets out the data breach management policy and forms part of the Council's Information Governance Policy Framework. The policy aims to ensure that Bolsover District Council reacts appropriately to any actual or suspected breaches of data protection.

The UK General Data Protection Regulation (UK GDPR) Article 5 states that data should be 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').

The Council is required to report certain types of personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. The Council must report incidents where there is a risk to people's rights and freedoms; this means that there are potential negative consequences for individuals because of a breach.

In practice, this means that the Council must have appropriate security to prevent the personal data we process being accidentally or deliberately compromised. This includes having the right physical and technical security, backed up by robust policies and procedures and well-trained and reliable staff. It also means that the organisation should be ready to respond to any threat to or breach of information security swiftly and effectively and have procedures in place to support that.

2. Scope and applicability

This policy is applicable to Council employees, Councillors, temporary and agency staff and contractors working for and on behalf of the Council and any organisations processing data on the Council's behalf.

It covers all data that is processed by the Council, i.e. all data that is obtained, held or stored, used, shared, retained or destroyed by the Council, and any data processed by a third-party organisation on behalf of the Council (i.e. under a contract).

It covers data in all formats and on all types of media, including paper-based information and documents, digital and electronic information, whether held on the Council's network, at off-site storage, a portable device, in the cloud or in transit.

This policy does not set out the Council's approach when responding to security incidents because of technical failures and/or cyberattacks. This can be found in the Council's **Joint Information and Cyber Security Policy (April 2024)**.

3. Data breaches defined

A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate actions, and it is more than simply 'losing' personal data.

Broadly speaking, where the confidentiality, integrity or availability of personal data has been affected a security incident has occurred.

Examples of data breaches include:

- IT equipment containing personal data being lost or stolen.
- Paper files being lost or stolen.
- Sending data to an incorrect recipient.
- Deliberate action where data taken without authorisation.
- Deleting data before it has reached its retention date.
- Altering personal data without authorisation.

In certain circumstances, the Council has a requirement to report the incident to the ICO within 72 hours.

4. Management of data breaches

Recital 87 of the UK GDPR states that organisations must quickly establish whether a personal data breach has occurred and take steps to address any breach which includes reporting to the ICO if required. Therefore, it is essential that that all breaches are reported to the Information and Engagement (I&E) team as soon as possible.

It is the responsibility of all members of the organisation, including those working on our behalf, to be aware of what constitutes a data breach and the action that needs to be taken in the event of a breach.

Following a data breach, the Council will take steps to contain the breach which includes ensuring that the right people and organisations are notified as soon as possible. Staff have a responsibility to report breaches as they become aware so that the Council can proactively manage the incident.

4.1 Immediate steps to be taken by staff

On becoming aware of a data breach, staff must:

►Report the breach via the following link: https://www.bolsover.gov.uk/data-protection-cctv-and-foi/report-a-data-breach
►Inform their line manager of the breach.
►Comply with any instruction/s from the I&E team.

4.2 Breach management by the I&E team

On receipt of a data breach report, the I&E team will work with the relevant service area to complete the security incident checklist. Following this initial assessment, the I&E team will determine whether the breach should be categorised as 'near miss', low risk or high risk.

The I&E team will work with the service area to contain the incident as far as possible. Immediate rectification actions to mitigate the incident will be provided to the reporting officer, such as asking an incorrect recipient to delete an email beyond retrieval.

The I&E team will escalate incidents to the Data Protection Officer (DPO) or Deputy Data Protection Officer (DDPO) as appropriate. The I&E team is responsible for leading the review of all data protection incidents and will work with the relevant service areas to identify:

■What personal data has been compromised.
■Whether personal data has been inappropriately accessed.
■How the incident can be contained (limiting or restricting further impact of the incident).
■The risk of harm or distress to individuals whose data has been compromised (the data subjects).
■If and/or how data subjects will be told, or 'notified' of the incident.
■How the incident occurred.
■Any weaknesses in the Council's processes, procedures, organisational or technical controls which may have led or contributed to the incident.
■What mitigating actions or controls are required to increase resilience, to prevent or reduce the likelihood or a reoccurrence, or to reduce the impact of any reoccurrence.

The I&E team maintain a register of all breaches and provide details on the number of data breaches and near misses to the SLT. Additionally, the I&E team provide details on the number of serious incidents that have been reported to the ICO as part of the Council's assurance statements.

For all incidents escalated to the DPO/DDPO (i.e. all except near misses), the following approach will be adopted.

4.2.a Containment and recovery

✓The DPO/DDPO shall be alerted to the breach immediately.
✓Any steps to prevent any further breach of the data will be implemented.
✓The DPO/DDPO will immediately notify the SIRO, relevant director and service manager. *Where an incident is very high risk, the Chief Executive Officer will also be notified.*

✓If known from the initial assessment, the DPO/DDPO will provide a recommendation on notification to the ICO and where necessary, will involve the SIRO.
✓The I&E team will alert the Communications team to ensure any media attention can be proactively managed.
✓The I&E team will ensure that Legal Services are notified of serious incidents who will manage any legal action taken against the Council because of a serious incident.
✓The I&E team will convene a meeting with the relevant service managers to review the incident and assess the risk against individuals.
✓The I&E team will identify whether any other organisations have been affected and notify them accordingly.
✓For breaches involving other governmental bodies such as DWP or NHS, further notification will be required as set out below.

4.2.b Assessment of risk

The I&E team will carry out an initial assessment of the risk to the rights and freedoms of individuals and agree the risk level (near miss, low or high). Where necessary, a formal likelihood-versus-impact assessment will be conducted with the relevant service area.

The assessment will always consider the potential impact on individuals' rights and freedoms and the likelihood of that impact occurring. A breach must be reported to the ICO if it is likely to result in a risk to individuals' rights and freedoms (even if the overall risk is assessed as low).

Notification to individuals is required only where the risk is high. The I&E team will work with the service area to carry out the risk assessment based on the following criteria:

■ The type of breach – this may affect the level of risk to individuals.
■ The nature, sensitivity and volume of personal data – the more sensitive the data, the higher the risk of harm (context will always be considered).
■ Ease of identification – encrypted or pseudonymised data reduces the likelihood of identification.
■ Risk of harm to the individuals – physical harm, theft, fraud, psychological distress, humiliation or damage to reputation.
■ Vulnerability of the individuals – for example, children or other vulnerable groups.
■ Number of individuals affected – generally the higher the number, the greater the impact (context will always be taken into consideration).

4.2.c Notification of the breach

The Information Commissioner's Office (ICO)

Where the risk assessment identifies that the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO/DDPO will recommend to the SIRO that the breach is reported to the ICO. The Council will report without

undue delay and, where feasible, not later than 72 hours of becoming aware of the breach. Only breaches assessed as unlikely to result in any risk to individuals' rights and freedoms are exempt from notification (this decision must be documented).

Department of Work and Pensions

In cases where it is identified that DWP information has been breached, the I&E team will report the breach to the DWP's DPO.

NHS Digital

All incidents (regardless of severity) involving Health and Social Care data must be reported by the I&E team via the NHS Data Security and Protection Incident Reporting tool. This will report incidents to the NHS Digital, Department of Health, ICO and other regulators.

Individuals

Where it has been identified that individuals should be notified of the breach, correspondence will be sent via the accountable Director for the affected service. The DPO/DDPO will provide support with wording for the letters/emails and any recommended protective steps for individuals.

4.2.d Evaluation and response

The I&E team will document all findings in a report, which will include:

■Details of the breach and how it occurred.
■The risk assessment of the incident and subsequent recommendation of reporting to the ICO.
■Risk assessment and recommendations around notification of individuals.
■Outline training completed by members of staff.
■Recommendations and actions that should be taken to mitigate the breach occurring in the future.

The report will be shared with the SIRO, CEO, and relevant Director.

5. Section 170 Offences, Data Protection Act

Section 170 (s170) of the Data Protection Act 2018 sets out a criminal offence in relation to individuals unlawfully obtaining personal data. Specifically, s170 states that it is a criminal offence for an individual to:

■Knowingly or recklessly obtain, disclose or procure personal data without the consent of the data controller.
■Sell data that was obtained unlawfully.
■Recklessly retain personal data – even if it was obtained lawfully – without the consent of the data controller.

If it is suspected that a member of staff has committed a s170 offence, the breach must be reported in the usual manner and investigated by the I&E team.

If a I&E-led investigation identifies that a member of staff has likely committed a s170 offence under the Data Protection Act 2018, the above process will be followed to assess the risk, and the following will also occur:

►HR to be notified immediately so that advice can be taken on disciplinary action.
►The ICO to be contacted to seek their advice on notification.
►Whether the breach is so serious that a report needs to be made to the Police.

In serious cases where s170 offences have occurred, the I&E team will report the matter to the ICO who will determine whether they wish to prosecute the individual for the offence.

6. Security incidents

The ICT team will lead on the technical response for any cyberattack that has affected Council systems.

For serious breaches that are a result of a technical failure, an incident manager will be identified by the SIRO. The incident manager will be responsible for overseeing the Council's response to the incident, ensuring that tasks are completed and will liaise with I&E team as required.

7. Third party data processors

Third party data processors who process personal data must be made aware of their responsibilities and their obligations to the Data Controller (the Council), and how to report a data breach or security incident.

Contracts with third parties who process personal data on behalf of the Council must include robust clauses to ensure that personal data is processed in accordance with the UK GDPR. The contract between the Council and the contractor provides the legal basis for the data processing, the categories of data being processed and sets out information security management procedures. Any breaches of data caused by a third-party processor must be reported in accordance with this policy.

For further information about Bolsover District Council's compliance with data protection law, please email GDPR@bolsover.gov.uk.

Appendix 4

Individual Rights Procedure
Data Protection – How to exercise your rights
UK GDPR and Data Protection Act 2018

2026

(Version 2.0 – April 2026, reflecting Data (Use and Access) Act 2025)

1. Summary

This procedure sets out how the Council will comply with the requirements of the data protection legislation in relation to the rights of individuals. It will inform you what your rights are, any restrictions on those rights and how to exercise those rights. It sets out the Council's responsibilities and shows how the Council will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and other regulations and good practice standards in relation to your rights (including changes from the Data (Use and Access) Act 2025).

2. Scope

This procedure applies to all data subjects who the Council processes information about. This includes employees as well as all service users and residents of Bolsover. It covers personal data we collect and use on paper and electronically including our computer databases and network, paper records, videos and photographs, voice recordings, CCTV and mobile devices such as laptops, mobile phones, memory sticks and pendant alarms.

3. Introduction

The law gives individuals (data subjects) several rights to control what personal information is given to the Council and how it is used by us.

The UK GDPR provides the following rights for individuals:

►The right to be informed
►The right of access
►The right to rectification
►The right to erasure (also known as the right to be forgotten)
►The right to restrict processing
►The right to data portability
►The right to object
►Rights in relation to automated decision making and profiling.

All the rights are detailed in this procedure. If you have any queries regarding any of these rights, please contact GDPR@bolsover.gov.uk.

Requests

If you wish to make a request to exercise any of the rights detailed in this procedure, this can be done verbally or in writing. However, it would help us to confirm and clarify the details if you could put the request in writing. If you are unable to do this, or would prefer not to, one of our staff will log the details and ask you to confirm their understanding of your request verbally.

If we require information to confirm your identity or to verify any of the details provided, we will contact you and request additional information.

We do not normally charge a fee for dealing with your request but in certain circumstances we may do so. This is only where we would consider a request to be unfounded or excessive (especially repeat requests) and we would inform you of any charge before proceeding with your request.

The law requires that any communications we provide to you regarding your rights must be clear and transparent using plain language. If you receive any information which is not clear, please contact GDPR@bolsover.gov.uk and we will ensure further explanations are provided to you.

Where you correspond with us by electronic means (such as email) we will normally respond by the same method unless you advise otherwise.

To exercise any of the rights in this procedure please email GDPR@bolsover.gov.uk or write to the Data Protection Officer, Bolsover District Council, The Arc, Clowne, S43 4JY.

Response Times

We will respond within one month of receipt. We may "stop the clock" (pause the one-month period) while we reasonably seek clarification from you about the scope of your request or to verify your identity. We will tell you if this happens and when the clock restarts.

The period may also be extended by up to two further months if the request is complex or we receive several similar requests; we will notify you within the first month and explain the reasons.

Where we decide not to action a request, we will inform you why. If you disagree with our decision, you have the right to complain to the Information Commissioner's Office. Their contact details are on their website at: ico.org.uk

4. The Right to be Informed

When we collect information from you, you have the right to be told what we are going to do with that information. We will tell you what we will use your data for, how long we will keep it, who we may share it with, and the other details listed below.

This information will usually be provided to you in a **Privacy Notice**.

The information in the notice must be concise, transparent, intelligible, easily accessible and written in clear and plain language. There are full details regarding privacy notices on our website at https://www.bolsover.gov.uk/privacy.

Where we collect information from you, we will provide the details listed below (see the privacy page detailed above for further information about different services and the information they use):

1. The identity and contact details of the data controller (Bolsover District Council)
2. The contact details to reach the Council's Data Protection Officer
3. The reasons why we use your information
4. The legal reason for processing your information
5. Any people or organisations who we share information with or disclose data to
6. Any transfers of information to certain countries or international organisations (the Council is unlikely to make any international transfers, but we will inform you if we think this is applicable)
7. How long we will keep your information
8. Advise you of your rights in relation to your information (as detailed in this procedure)
9. Advise you of your right to complain to the Information Commissioner's Office
10. We will inform you where it is a statutory requirement to provide information (i.e. where there is a law in place which means you must provide the information, e.g. for Council tax purposes) or we require the information for a contractual requirement. We will also inform you of the implications of not providing the information, i.e. what actions the Council may take
11. If any automated decisions (i.e. decisions made by a computerised system) are made or we use any profiling (automated evaluation of personal information used to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, or similar matters).

If we collect data about you from a third party (i.e. anyone other than you) we will let you know and give you the information listed above as well as details of the categories of personal data we hold (such as your name, address, employment history etc.) and tell you who provided the data to us.

We will not provide this information every time you contact us, but we will do so where you apply for a new service or contact a different department.

5. The Right of Access

You have the right to ask for copies of the personal information the Council holds about you. This is called a Subject Access Request (SAR).

Subject Access Requests

Requests can be made to the Council verbally or in writing. However, we would normally ask you to put the request in writing so that we can confirm who you are, and we have a written record of your request. You can submit a SAR by visiting our website; this is the easiest, most efficient way to submit your request.

You may also email GDPR@bolsover.gov.uk or phone 01246 242424 to provide your details verbally.

When you submit your request, the GDPR Team will send you a written acknowledgement, log it and forward it to the relevant service area to provide a response.

The response will normally be sent within one month of receipt of the request.

We carry out a reasonable and proportionate search of the relevant systems and records (we are not required to search every system exhaustively).

We will need to ask you for further information to confirm your identity or to trace the information you want.

What Information can be provided?

You are entitled to ask for any information the Council holds about you. We will carry out a reasonable and proportionate search to locate it.

The Council holds a large volume of data in several departments and on different systems so it would help us find the information if you could provide details of departments or staff you have dealt with, services you have requested or any reference numbers the Council has given you.

Once you have told us what information you require, we will search the relevant files and extract all the information that relates to you. Information about other people will be removed unless we think you would already know this information, or you provide consent from the other individuals to disclose their information.

There are some circumstances where the information will be exempt from the right of subject access. For example, if the disclosure would prejudice a criminal investigation. If this applies, we will inform you when we respond to your request.

CCTV Footage

If you request a copy of any CCTV footage you will only be entitled to images of yourself. Images of other people or vehicles will be removed. Therefore, if you are requesting this information because you want evidence of an incident or accident you should ask the police or your insurance company to make an official request for information. We may be able to provide footage of the full incident directly to them under one of the exemptions within the data protection legislation. This enables the Council to provide more information for the purpose of an official investigation or claim.

6. The Right to Rectification

If you believe we hold information about you which is inaccurate or incomplete you can ask us to rectify (i.e. correct) the information or complete it if it is incomplete. Where such a request is received, we will review the contested information and the details you have provided and decide whether we need to change or complete the information held.

If the information contested is sensitive and / or will be used to make decisions affecting you, we will consider restricting use of the data until the matter is resolved. After reviewing your request, we will inform you of our decision and detail the reasons for the decision. If you disagree with our decision, you can complain to the ICO.

7. The Right to Erasure

In some circumstances you can ask for your information to be erased / deleted under the UK GDPR.

You have this right where:

■It is no longer necessary for us to hold the information for the purpose for which it was originally collected / processed
■You withdraw your consent for us to hold this information and the only legal reason we had to process it was because you had consented
■You object to the processing of your information, and we have no overriding legitimate reasons to allow us to continue using your information
■You object to the Council using your information for marketing purposes
■Your information has been unlawfully processed by the Council or has to be erased to comply with a legal obligation (e.g. to comply with a court order); or

This right will not apply if the information is processed:

●to exercise a right of freedom of expression and information
●to comply with a legal obligation or for a task carried out in the public interest or in the exercise of the Council's official authority
●for establishing, exercising or defending legal claims; or
●for certain purposes relating to public health, for archiving in the public interest, scientific/historical research or statistical purposes.

Where we agree to delete information and have disclosed the data to third parties, we will inform them about the erasure of the personal data.

If the information has been made public (e.g. published on a website) and we are obliged to erase it, we will make all reasonable steps to delete the data and ensure other data controllers delete the data. Reasonable steps will include any technical measures, taking account of available technologies and the costs of implementation.

8. The Right to Restriction of Processing

You have the right to ask the Council to restrict the processing of your personal data where:

○You have contested the accuracy of the information and are waiting for us to respond or change the information
○you have objected to the processing, and we are considering whether we have a legitimate reason to process your information which overrides this
○the processing is unlawful, but you would prefer the Council to restrict the data rather than erase it
○the Council no longer needs the data, but you require it to establish, exercise or defend a legal claim.

If we have disclosed the personal data to third parties, then we must inform them about the restriction of the personal data. Where processing has been restricted, we will inform you before the restriction is lifted.

9. The Right to Data Portability

The right to data portability allows individuals to move, copy or transfer personal data easily from one ICT environment to another in a safe and secure way.

This right is primarily for commercial use and will enable individuals to take advantage of applications and services which can use this data to find them a better deal, help them understand their spending habits or move suppliers quickly and easily.

Where this right applies, we must provide the personal data to you in a structured, commonly used and machine-readable form (e.g. CSV files). If you request it, we may have to transmit the data directly to another organisation if this is technically feasible.

The right to data portability only applies to personal data you have supplied to the Council, where the only legal reason we have for processing the information is that you have consented, or you have given us the information for a contractual arrangement and the processing is carried out by automated means.

The right to data portability does not apply if information is being processed for a task carried out in the public interest or in the exercise of the Council's official authority.

It is unlikely that any Council services will be covered by this right. However, if you think it applies to any of your information, please contact GDPR@bolsover.gov.uk and we will consider your request and respond to you detailing our decision.

10. The Right to Object

You have the right to object to the Council processing your data where:

~the reason for processing is based on legitimate interests, the performance of a task in the public interest or the exercise of official authority (including profiling)
~processing is for direct marketing (including profiling); and
~processing is for certain scientific/historical research or statistical purposes.

Where you object to us using your information for direct marketing we will stop using the data for this purpose immediately.

Where you object to our processing your personal data other than for direct marketing, we must comply with your request unless we can show you overriding compelling legitimate grounds to continue processing or that the processing is for the establishment, exercise or defence of legal claims.

11. Rights relating to Automated Decision Making and Profiling

Where the Council uses automated decision making (i.e. where a decision is made by computerised means such as credit scoring) or profiling (automated evaluation of personal information used to analyse or predict their performance at work, economic situation, health, personal preferences, reliability, or similar matters), and that decision could affect you or another individual, you have the right to:

●ask for human intervention to review a decision that has been made automatically
●express your point of view; and
●obtain an explanation of the decision and challenge it.

The right does not apply if the automated decision:

■is necessary for entering into or performance of a contract between you and the Council
■is authorised by law (e.g. for the purposes of fraud or tax evasion prevention)
■is based on explicit (i.e. clearly given and understood) consent.

If the Council processes personal data for profiling purposes, we will ensure that appropriate safeguards are in place. For example, we will tell you about the logic involved in decisions (i.e. how calculations are made) and we will have measures in place to correct inaccuracies and reduce the risk of errors.

Complaints

If you are unhappy with how we have handled your personal data or any request under this procedure, you may complain directly to us. We will acknowledge your complaint within 30 days and aim to resolve it without undue delay. (This becomes a statutory right on 19 June 2026.) You can also complain to the Information Commissioner's Office at any time: ico.org.uk.

To exercise any of the rights in this procedure please email GDPR@bolsover.gov.uk or write to the Data Protection Officer, Bolsover District Council, The Arc, High Street, Clowne, S43 4JY.

Appendix 5

Draft Redaction Policy 2026

1. Introduction

1.1 The Council is committed to transparency and openness in line with the Freedom of Information Act 2000, the Environmental Information Regulations 2004 and the Local Government Transparency Code 2015. Where information is exempt under data protection legislation, the common law duty of confidentiality or other legal obligations, it will be redacted or withheld prior to publication or disclosure.

1.2 This policy provides a clear, consistent approach to redaction across the Council. It protects personal and confidential information while enabling lawful disclosure.

1.3 The policy applies to all information published or disclosed by the Council (including on the website), all staff involved in publishing or disclosing documents, and all formats (hard copy and electronic). It covers personal data relating to living individuals and information subject to a duty of confidentiality.

2. Roles and Responsibilities

2.1 All staff responsible for publishing or disclosing information must receive training on redaction requirements, procedures and the use of approved software.

2.2 ICT will provide approved redaction software (currently Qoppa) to relevant staff. At least two licences per team are recommended.

2.3 The Information & Engagement team will provide advice and guidance, carry out redaction for FOI, EIR and SAR responses, and lead annual policy reviews.

3. What is Redaction?

Redaction is the term used to describe the editing process whereby information is removed from a document. This is done by blocking out individual words, a signature, sentence, paragraph or section, prior to the disclosure of information or a document.

4. Legal and Regulatory Requirements

4.1 The Council will comply with all relevant legislation, including:

- Common Law Duty of Confidentiality
- Data Protection Act 2018 (DPA)
- UK GDPR
- Environmental Information Regulations 2004 (EIR)
- Freedom of Information Act 2000 (FOIA).

4.2 Under UK GDPR, processing of personal data requires a lawful basis (Article 6) and, for special category or criminal offence data, an additional condition (Article 9).

4.3 Under FOIA and EIR, information must be disclosed unless an exemption applies. Where an exemption is engaged, the Information & Engagement team will conduct and document a public interest test.

4.4 An entire document may only be withheld if all information is exempt or redaction would render it meaningless. Staff must refer to the latest ICO guidance on “Disclosing documents to the public securely”.

5. Identifying Information for Redaction

5.1 The personal data of living individuals is protected under data protection legislation and must be redacted or withheld except in the circumstances set out in the Redaction Criteria table (Section 8).

5.2 Wherever the Council owes a duty of confidentiality, that information must be redacted or withheld except in the circumstances set out in the Redaction Criteria table. A public interest test may be required before withholding.

5.3 The Council may use its discretion to redact any comments or information considered derogatory or offensive. Publishing such comments (e.g. in planning representations) does not imply Council endorsement.

5.4 Staff must consult the Redaction Criteria table before publishing or disclosing any document.

6. Exceptions to Redaction

6.1 There are exceptions which permit personal data to be made available to the public, under Schedule 2, paragraph 5 of the Data Protection Act 2018, where disclosure of the data is required by an enactment. Significantly for the Council (as a planning authority), these exceptions include the names and addresses of planning applicants, as required under section 69 of the Town and Country Planning Act 1990.

6.2 In addition, there may be exceptional circumstances when personal information is not required to be redacted, which could relate to Planning or Governance criterions. This basis can also apply to senior officers, acting in their capacity of granting official or legal permissions. The Council will only publish personal information that is necessary and may include:

●Names, signatures and contact details of senior managers of Bolsover District Council (Deputy and Assistant Director and above) or other authorised signatories acting in their official capacity on behalf of the Council; and
●Names, signatures and contact details of senior third-party representatives (where it is clear they occupy a senior position), acting in their official capacity on behalf of their organisations.

6.3 There may be instances where third parties request that we publish personal information, to promote an initiative, for example, individuals representing an

allotment association. In which case, we will obtain and record an individual's written consent prior to publishing. The individual may withdraw their consent at any time, in which case their personal information will be removed immediately from the website.

6.4 There shall be a presumption that all information and documents provided by the Council to the Local Government Ombudsman and Social Care Ombudsman for the purpose of an investigation of a referred complaint will be provided in an unredacted form.

7. Undertaking Redaction

7.1 Redaction must only be carried out on a copy of the document. The original must be retained in accordance with the Retention Schedule.

7.2 Appropriate methods must be used to ensure redacted information cannot be recovered or inferred (including when the document is held to the light).

7.3 Redaction software (Qoppa or approved alternative) must be used correctly to produce irreversible redactions. All metadata, tracked changes, comments, hidden data and previous versions must be removed before publication.

7.4 Black highlighting must be used on white or pale backgrounds. White redaction must be avoided.

7.5 A two-person check process is **mandatory**: every redacted document must be reviewed and approved by a second person or line manager before publication or disclosure.

7.6 Whole sentences or paragraphs must not be removed unless necessary to protect the remaining text from revealing the redacted content. If heavy redaction renders a document meaningless, the entire document must be withheld.

7.7 Redactions must be consistent and logical throughout the document.

7.8 Information supplied to the Information & Engagement team for FOI, EIR or SAR responses must be provided unredacted; the team will apply all necessary redactions.

8. Redaction Criteria

We will seek to apply the following redaction criteria across the Council to protect personal and confidential information against unauthorised disclosure and to disclose relevant information appropriately and lawfully. It should be noted that under FOIA and EIR, some of the information categories below may be subject to an exemption and public interest test.

Information type	Details/examples	Reasons for redaction	Relevant legislation/exemption	Exceptions to redaction
Bank account details	Of individuals	Personal information	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	Data subject exercising their own right of access
Bank account details	Of businesses/commercial information	Confidential/commercial information	Common law; FOIA s.41; FOIA s.43	None
Details of contractual arrangements	With external providers	Confidential information	Common law; FOIA s.41; FOIA s.43	None
Criminal offence data	Any information in connection with an offence	Personal information	DPA 2018 / UK GDPR Art 10; FOIA s.40	Data subject exercising their own right of access
Date of birth	Including day, month or year or any combination	Personal information	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	Data subject exercising their own right of access
Home address	All lines of an individual's home address, including postcode	Personal information	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	• Home addresses of planning applicants (TCPA 1990 s.69 registers) • Data subject exercising their own right of access
Legal communications	Information relating to legal proceedings	Confidential information	Common law; FOIA s.41; FOIA s.42	None

Name	All first, middle and last names and nicknames.	Personal information	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	• Names of planning applicants • Licensees on Licensing registers • Data subject exercising their own right of access • Senior Bolsover District Council staff (Deputy and Assistant Directors and above) and authorised signatories • Senior third-party representatives acting in official capacity • Names of junior officers in published minutes of public meetings
Personal email addresses	Also, any part of a business email address that includes an individual's name.	Personal information	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	• Data subject exercising their own right of access • Senior Bolsover District Council staff (Deputy and Assistant Directors and above) and authorised signatories • Senior third-party representatives acting in official capacity
Personal telephone numbers	Including landline and mobile	Personal information	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	Data subject exercising their own right of access
Pronouns/Title	In relation to redacted names	Personal information (to prevent inference)	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	Relating to senior staff or senior third-party

	(her/his, he/she), Ms/Mrs/Miss/Mr, etc.			representatives acting in official capacity
Protected species and their sites	Information from Environmental Impact Assessments (EIAs) or similar planning documents	Protected species information	EIR reg 12(5)(g); Wildlife & Countryside Act 1981	Planning inspection (where required)
Sensitive personal information (special category)	Racial or ethnic origin, political opinions, religious beliefs, trade union membership, biometric data, etc.	Special category personal information	DPA 2018 / UK GDPR Art 9; FOIA s.40	Data subject exercising their own right of access
Signatures	Handwritten and electronic	Personal information	DPA 2018 / UK GDPR Art 5 & 6; FOIA s.40	Data subject exercising their own right of access • Senior Bolsover District Council staff (Deputy and Assistant Directors and above) and authorised signatories • Senior third-party representatives acting in official capacity

9. Compliance

9.1 All staff responsible for publishing and disclosing information and documents must comply with this Redaction Policy.

9.2 Failure to comply with this Redaction Policy may result in financial loss or reputational harm to individuals, businesses, organisations and the Council.

10. Review

This policy will be reviewed at least annually by the Information & Engagement Manager and the Council's SIRO, or sooner if there is a significant change in legislation or ICO guidance.

11. Related Policies

This policy must be read in conjunction with the Council's Data Protection Policy and all other relevant/associated policies.

2026 Data Protection Complaints Procedure

Bolsover District Council is committed to protecting personal data and upholding individuals' rights under data protection law, including the Data Protection Act 2018, UK GDPR (as amended), and the Data (Use and Access) Act 2025.

This procedure sets out how we handle data protection complaints and meets our legal obligation to provide a clear process for individuals to complain directly to us.

Scope

This applies to complaints about our handling of personal data, including (but not limited to):

- Subject Access Requests
- Data incidents or breaches
- Misuse or unfair processing of personal data
- Retention or accuracy of data
- Profiling or automated decision-making

Complaints from children/young people

We will speak directly with children or young people (where appropriate) to ensure they understand their complaint.

Third-party complaints

If the complaint is made on behalf of someone else or concerns a child/young person where the complainant does not have parental responsibility, we may not accept it as it could involve third-party personal data.

In appropriate cases we may still investigate, but the complainant will not receive details of the outcome unless we have written consent from the affected individual.

Our three-stage process

1. Local Resolution

We will contact you within two working days (by phone, email or letter) to acknowledge your complaint and confirm when you can expect a full written response. We will keep you updated on progress.

This is normally within one month of acceptance. If we need to extend this, we will contact you with an explanation.

2. Complaint Review

If you are not satisfied with the outcome, you may request a review within 20 working days of receiving our response.

• We will acknowledge your review request within two working days.
• An independent officer (not involved in the original decision) will review it.
• You will be asked why you are unhappy and may provide additional evidence.
• We aim to respond within one month. If we need to extend this, we will explain why in a timely manner.

3. Information Commissioner's Office (ICO)

If you remain dissatisfied after the review, you have the right to complain to the ICO at any time (you do not need to complete our internal process first).
Contact details: https://ico.org.uk/make-a-complaint/data-protection-complaints/

How to make a data protection complaint

You can complain verbally or in writing (any format), either separately or as part of other correspondence.

Send complaints to:

Email: GDPR@bolsover.gov.uk
Post: The Information & Engagement Team, Bolsover District Council, The Arc, High Street, Clowne, S43 4JY

Confidentiality

Information about your complaint is confidential and shared only with those directly involved in the investigation.