Data Protection Policy

2026

Last reviewed: April 2026 (Updated to reflect the Data (Use and Access) Act 2025)
Next review due: April 2028 (or sooner if there are significant changes to data protection legislation)

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) supported by the Council's Data Protection Officer. Regular internal audits and reporting to senior leadership will be conducted to ensure ongoing adherence.

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.
● ICO Guidance on Recognised Legitimate Interest: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/recognised-legitimate-interest/

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

27. Policy Review

This Policy will be reviewed every two years or sooner if required by changes in legislation, ICO guidance or operational needs.

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