



RIPON CITY COUNCIL

Data Protection Policy

Item	Detail
Adopted by Full Council	June 29, 2026
Previous version	June 5, 2018 (Pre GDPR)
Current update	June 23, 2026
Date of review	2028

Introduction

Ripon City Council needs to collect and use personal information about residents, service users, employees, councillors, contractors, volunteers, hirers, consultees, suppliers, correspondents and other people who come into contact with the Council. The Council will only collect and use personal information where it has a lawful reason to do so and will handle it fairly, securely and transparently.

This policy explains how Ripon City Council will comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003 (PECR), and the Data (Use and Access) Act 2025 (DUAA), as those laws apply from time to time.

The DUAA amends, but does not replace, the UK GDPR, Data Protection Act 2018 and PECR. The Council will review this policy and its procedures as further DUAA provisions, commencement regulations and Information Commissioner guidance take effect.

This policy applies to personal information held electronically, on paper, in audio or video form, on websites or online platforms, in email accounts, within third-party systems, or on any device used for Council business.

Definitions

Term	Meaning
Personal data	information relating to an identified or identifiable living individual. This includes names, addresses, email addresses, telephone numbers, photographs, online identifiers and any other information that can identify a person directly or indirectly.
Special category data	more sensitive personal data, including information about health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric data used for identification, sex life or sexual orientation.
Criminal offence data	personal data relating to criminal convictions, offences, allegations, proceedings or related security measures.
Data subject	the living individual whose personal data is being processed.
Processing	anything done with personal data, including collecting, recording, storing, using, sharing, disclosing, deleting or destroying it.
Data controller	the organisation that decides why and how personal data is processed. Ripon City Council is the Data Controller for personal data processed for Council purposes.
Data processor	an organisation or person that processes personal data on behalf of the Council, such as an IT, website, payroll, survey, mailing-list or records-management provider.
Data protection lead	the officer nominated by the Council to oversee day-to-day data protection compliance and act as the first point of contact for data protection enquiries.
Consent	a freely given, specific, informed and unambiguous indication by which a person agrees to the processing of their personal data. Consent must involve a clear positive action and can be withdrawn.
Direct marketing	the communication, by any means, of advertising or marketing material directed to particular individuals. This may include invitations, promotional material, fundraising or public engagement communications where the law treats them as direct marketing.

Data Controller and responsibility

Ripon City Council is the Data Controller for personal data processed for Council purposes. The Council is responsible for ensuring that personal data is handled in accordance with data protection law.

The Chief Officer, or another officer nominated by the Council, will act as the Council's data protection lead unless the Council appoints a separate Data Protection Officer or external adviser. Contact details will be published on the Council website and in relevant privacy notices.

All councillors, employees, contractors and volunteers who handle personal data for Council purposes must follow this policy and any related Council procedures. Councillors must take particular care where they use personal devices, personal email accounts or personal storage for Council business.

Data protection principles

Ripon City Council will comply with the data protection principles. Personal data shall be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used in a way that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than is necessary;
- processed securely, using appropriate technical and organisational measures; and
- handled in a way that allows the Council to demonstrate compliance.

Lawful bases for processing

The Council will identify and record a lawful basis before processing personal data. The lawful basis will depend on the purpose. The Council may rely on:

- legal obligation, where processing is needed to comply with a legal duty;
- public task, where processing is needed to perform a task in the public interest or exercise official authority;
- contract, where processing is needed for a contract or steps before entering into a contract;
- consent, where a person has clearly opted in and can withdraw consent;
- vital interests, where processing is needed to protect someone's life; or
- legitimate interests, only where the law permits its use and not where the Council is processing in the performance of its public tasks.

Where special category data is processed, the Council will also identify a separate condition under Article 9 UK GDPR and, where required, a condition in the Data Protection Act 2018. Where criminal offence data is processed, the Council will only do so where authorised by law and subject to appropriate safeguards.

Collecting personal data and privacy information

When collecting personal data, the Council will explain clearly why the information is needed, how it will be used, the lawful basis, who it may be shared with, how long it will be kept, and what rights the individual has. This will normally be done through a privacy notice, wording on a form, website text, or direct communication with the individual.

The Council will not collect more personal data than is necessary for the relevant purpose. Forms, surveys and online sign-up processes must be reviewed before use to ensure that unnecessary questions are not included.

Where the Council relies on consent, consent wording must be separate, clear and specific. Pre-ticked boxes, silence, inactivity or bundled consent will not be treated as valid consent.

Public mailing list and electronic communications

Ripon City Council may operate a public mailing list to provide updates about Council news, consultations, events, heritage projects, community engagement, civic activity and other matters of public interest.

Individuals will normally only be added to the mailing list where they have actively chosen to subscribe, for example by completing an online sign-up form on the Council's website or by otherwise giving clear consent. The Council will not add individuals to the public mailing list merely because they have contacted the Council, attended an event, completed a survey, submitted feedback, or corresponded with councillors or officers, unless they have separately opted in.

The lawful basis for the public mailing list will normally be consent. The Council will keep evidence of consent, including via sign-up wording they were shown at the time of sign-up.

Every mailshot must clearly identify Ripon City Council and include a simple way to unsubscribe or opt out. Where a person withdraws consent or objects to mailing-list communications, the Council will endeavor to stop sending such communications and may retain a minimal suppression record to avoid contacting them again in error.

The Council will not use its public mailing list for party-political purposes, electioneering, or purposes unrelated to the sign-up wording. Mailing-list data must not be shared with councillors, third parties or partner organisations unless there is a clear lawful basis and privacy information has been provided.

The Council will treat electronic mailshots and similar communications with care under PECR. Where a communication may amount to direct marketing, the Council will ensure that PECR requirements are met before it is sent.

The Council notes that the DUAA introduced a specific charity soft opt-in for certain charitable electronic mail marketing. Ripon City Council will not rely on that charity soft opt-in for the Council's own public mailing list, because the Council is not a charity. Any separate charity connected with Council projects must have its own privacy arrangements and must not automatically receive the Council's mailing-list data.

Online forms and third-party platforms

The Council may use third-party online services, including SurveyMonkey, to collect mailing list sign-ups, issue surveys, manage online forms, analyse responses and/or send electronic communications.

Where a third-party provider processes personal data on the Council's behalf, the Council remains responsible for compliance. Before using such a provider, the Council will take reasonable steps to ensure that appropriate data processing terms, security arrangements, access controls and retention arrangements are in place.

Website sign-up forms and embedded forms must be accompanied by clear privacy wording. The Council will avoid using unnecessary tracking, profiling or intrusive pop-ups unless these have been reviewed for data protection, PECR and cookie compliance.

Access to SurveyMonkey or any equivalent system must be limited to authorised officers. Personal data should not be exported, downloaded or retained separately unless necessary for a Council purpose and stored securely.

Surveys, consultations and engagement

The Council may collect personal data through surveys, consultations, public meetings, events and engagement activity. The Council will be clear whether responses are anonymous, confidential, or attributable to a named person.

Survey responses will not be used to add people to a mailing list unless the individual has separately opted in. Where consultation results are reported to councillors or published, personal data will be anonymised or minimised unless there is a lawful reason to identify individuals.

Where children or young people may complete forms, enter competitions or use online services, the Council will consider their needs and ensure information is clear, age-appropriate and proportionate. The Council will consider whether parental or carer consent is needed for the particular activity.

Sharing and disclosure

The Council may share personal data where it is lawful and necessary, including with local authorities, public bodies, emergency services, auditors, insurers, legal advisers, IT providers, payroll and pension providers, contractors, grant funders, regulators and partner organisations.

Personal data may be disclosed without consent where the law allows or requires it, including where disclosure is needed to comply with a legal duty, protect vital interests, prevent or detect crime, obtain legal advice, conduct legal proceedings, respond to safeguarding concerns, support audit or regulatory functions, or perform a public task.

The DUAA clarifies some circumstances in which personal data may be disclosed to help another organisation perform its public tasks. The Council will still check that any disclosure is necessary, proportionate and recorded.

Data sharing arrangements must be documented where appropriate, particularly where sharing is regular, systematic, sensitive, or involves special category or criminal offence data.

International transfers

Some third-party providers may process or store personal data outside the United Kingdom. Where this happens, the Council will ensure that appropriate safeguards are in place, such as adequacy arrangements, standard contractual clauses, an international data transfer agreement, or another lawful transfer mechanism. The Council will review provider information where relevant, including sub-processors and hosting arrangements.

Data subject rights

Individuals have rights under data protection law. These include, subject to conditions and exemptions:

- the right to be informed about how their personal data is used;
 - the right of access to their personal data;
 - the right to rectification of inaccurate data;
 - the right to erasure in certain circumstances;
 - the right to restrict processing in certain circumstances;
 - the right to object to certain processing;
 - the right to data portability in limited circumstances;
 - rights relating to solely automated decision-making where it has legal or similarly significant effects;
- and

- the right to complain to the Council and to the Information Commissioner.

Requests to exercise data protection rights must be passed promptly to the data protection lead. The Council will respond within the statutory timescale unless an extension or lawful exemption applies.

Subject access requests

A subject access request is a request by an individual for access to their own personal data. A request does not need to use any particular wording and may be made verbally or in writing.

The Council will respond to subject access requests within one month unless the law allows an extension. The DUAA clarifies that the Council is required to make reasonable and proportionate searches when responding to such requests. Where further information is reasonably needed to identify the requester, locate the information or clarify the request, the Council may pause the response time in accordance with the law until that information is received.

The Council will consider third-party information, confidentiality, legal professional privilege, management information, regulatory exemptions and other relevant exemptions before disclosure.

Complaints

The Council will make it easy for people to complain about how their personal data has been handled, including by providing an email address or other electronic route for complaints.

In line with the DUAA, the Council will acknowledge data protection complaints within 30 days and respond without undue delay. The Council will explain the outcome of the complaint and, where appropriate, any steps taken or proposed.

Individuals may also complain to the Information Commissioner's Office. The Council will include ICO contact details in its privacy information or correspondence where appropriate.

Security

The Council will take appropriate technical and organisational measures to keep personal data secure. These may include access controls, strong passwords, multi-factor authentication where available, secure storage, locked filing, encryption where appropriate, secure disposal, staff training, supplier checks and limits on who can access personal data.

Personal data must not be stored on personal devices, personal cloud storage or personal email accounts unless there is a clear Council-approved reason and suitable safeguards are in place. Where councillors or staff use personal devices for Council business, they must take reasonable steps to keep Council data separate, secure and retrievable for Council purposes.

Paper records containing personal data must be stored securely and disposed of by shredding or confidential waste arrangements. Electronic records must be deleted securely when no longer required. Equipment leaving Council control must be wiped or destroyed so that personal data is not recoverable.

Personal data breaches

A personal data breach is a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. Examples include emails sent to the wrong person, lost papers, lost devices, unauthorised access, cyber incidents, or accidental publication of personal data.

All suspected breaches must be reported immediately to the Chief Officer or data protection lead. The Council will assess the risk, take steps to contain the breach, record the incident, and decide whether it must be reported to the Information Commissioner and/or affected individuals.

Where a breach must be reported to the Information Commissioner, the Council will do so without undue delay and, where feasible, within 72 hours of becoming aware of it. If notification is later than 72 hours, the Council will record the reasons for the delay.

Retention and disposal

The Council will keep personal data only for as long as necessary for the purpose for which it was collected, including any legal, audit, financial, insurance, safeguarding, historical or public accountability requirement.

The Council will maintain or adopt a records retention schedule. When records reach the end of their retention period, they will be securely deleted, destroyed, anonymised or archived where appropriate.

Mailing-list data will normally be kept while the person remains subscribed. If a person unsubscribes, the Council may retain a minimal suppression record to ensure that they are not contacted again in error.

Automated decision-making and profiling

The Council will not use solely automated decision-making that has legal or similarly significant effects on individuals unless it has identified a lawful basis and provided the safeguards required by law. These safeguards may include giving individuals information about the decision, enabling them to make representations, allowing them to challenge the decision, and providing human intervention where required.

The Council will not use mailing-list, survey or website data for intrusive profiling or automated targeting unless this has been specifically reviewed and explained to individuals.

Cookies, analytics and website technologies

The Council will manage cookies and similar technologies in accordance with PECR and data protection law. Where consent is required, the Council will obtain valid consent before setting non-essential cookies or similar technologies.

The DUAA permits some low-risk storage and access technologies without explicit consent in certain circumstances. The Council will not rely on any such exemption unless it has reviewed the purpose, privacy impact and any current ICO guidance.

Training, review and accountability

The Council will ensure that employees, councillors, contractors and volunteers who handle personal data receive appropriate guidance or training. The level of training will depend on the nature of their role and the sensitivity of the personal data they handle.

The Council will maintain appropriate records of processing activities, privacy notices, supplier arrangements, data sharing arrangements, consent records, breach records and decisions about higher-risk processing.

Where processing is likely to result in a high risk to individuals, the Council will complete a Data Protection Impact Assessment before the processing begins.

This policy will be reviewed at least every two years, or sooner if there are significant legal, operational or technological changes.

Related documents

- Privacy notices; (Adopted October 2018);
- Records Management & Document Retention Policy; (Adopted March 2025);
- Information security procedures; (For June 2026 Approval)
- Data breach procedure: The Council will handle personal data breaches in accordance with the UK GDPR, the Data Protection Act 2018 and current Information Commissioner's Office guidance.
- Subject access request procedure; the Council will handle subject access requests in line with UK GDPR, Data Protection Act 2018 and current ICO guidance.
- Website privacy and cookie notice; (Drafting for July '26);
- IT Policy (Adopted June 2026);
- Safeguarding policy where personal data relates to children or adults at risk; (Adopted June 2026)

Contact

In case of any queries, requests or complaints in relation to this policy, please contact:

Chief Officer / Data Protection Lead

Ripon City Council

Town Hall

Ripon

HG4 1DD

Telephone: 01765 604097

Email: admin@riponcity.gov.uk

Individuals may also contact the Information Commissioner's Office for advice or to make a complaint.