



## GDPR Policy

### **Purpose of the policy and background to the UK General Data Protection Regulation (UK GDPR)**

This policy provides information to councillors, employees, and the public about UK GDPR and updates any previous data protection policy and procedures to include the additional requirements of UK GDPR and the Data Protection Act 2018, which apply in the UK following the exit from the EU. The Government has confirmed that despite the UK leaving the EU, UK GDPR will still be a legal requirement. This policy explains the duties and responsibilities of the council and identifies the means by which the council will meet its obligations.

Under the legislation personal data must be processed lawfully, fairly, and transparently; collected for specified, explicit, and legitimate purposes; be adequate, relevant, and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security.

### **For data to be processed lawfully it must be processed based on one of the six lawful grounds specified in Article 6 of the UK GDPR:**

- **Consent:** The individual has given clear and explicit permission for their data to be processed.
- **Contract:** Processing is necessary to fulfil a contract or to take steps before entering into a contract.
- **Legal Obligation:** Processing is required to comply with the law.
- **Vital Interests:** Processing is necessary to protect someone's life.
- **Public Task:** Processing is necessary to perform a task in the public interest or in the exercise of official authority.
- **Legitimate Interests:** Processing is necessary for legitimate interests pursued by the data controller or a third party, provided it doesn't override the rights and freedoms of the individual.

Where information collected is sensitive (referred to as special category data under the UK GDPR) additional conditions apply to its lawful use due to its heightened privacy implications. Special category data includes information about:

- **Racial or ethnic origin**
- **Political opinions**
- **Religious or philosophical beliefs**
- **Trade union membership**
- **Genetic data**
- **Biometric data (for identification purposes)**
- **Health data**

- **Sex life or sexual orientation**

To process this type of data, an organisation must satisfy **two criteria**:

1. **General lawful basis for processing** (as outlined in Article 6 of the UK GDPR, such as consent or legal obligation).
2. **Specific additional conditions** under Article 9 of the UK GDPR and Schedule 1 of the Data Protection Act 2018.

**At least one of the following conditions must apply for processing special category data:**

1. **Explicit Consent**  
The individual has provided clear and explicit consent for the processing of their sensitive data.
2. **Employment, Social Security, or Social Protection**  
Processing is necessary to carry out obligations or rights in the context of employment law, social security, or social protection (e.g., workplace health checks).
3. **Vital Interests**  
Processing is necessary to protect someone's life where the individual is physically or legally incapable of giving consent.
4. **Not-for-Profit Organisations**  
Processing is carried out by a foundation, association, or similar body as part of legitimate activities for their members, provided appropriate safeguards are in place.
5. **Public Interest**  
Processing is necessary for reasons of substantial public interest based on UK law.
6. **Healthcare and Social Care**  
Processing is necessary for medical diagnosis, the provision of healthcare or treatment, or the management of health or social care systems.
7. **Public Health**  
Processing is necessary for public health reasons, such as preventing the spread of infectious diseases, provided safeguards are in place.
8. **Research and Statistics**  
Processing is necessary for scientific, historical research, or statistical purposes, provided it serves the public interest and appropriate safeguards are applied.

### **Identifying the roles and minimizing risk**

UK GDPR requires that everyone within the council must understand the implications of data protection and that roles and duties must be assigned. The Council is the data controller and may appoint a Data Protection Officer (DPO), but this is not a legal requirement. A council must adhere to the issuing of clear and accessible privacy statements, deal with requests and complaints raised, and ensure the safe disposal of information. The Council will ensure information held is appropriately audited and managed.

As part of minimizing risks associated with data processing, the Council will conduct and maintain Data Protection Impact Assessments (DPIAs) for any high-risk processing activities, particularly those involving biometric data, surveillance, or other sensitive personal information.

GDPR requires continued care by everyone within the council, councillors, and employees, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the council facing a fine from the Information Commissioner's Office (ICO) for the breach itself and to compensate the individual(s) adversely affected. Therefore, handling information is a high/medium risk to the council (both financially and reputationally) and must be included in the Council's Risk Management Policy. This risk can be further minimized by avoiding the use of "dark patterns," such as pre-checked consent boxes or deceptive consent prompts, in all council digital interfaces to ensure fair and transparent data practices.

### **Data breaches**

Personal data breaches should be investigated. Investigations must be undertaken within one month of the report of a breach. In cases where a breach is likely to result in a risk to the rights and freedoms of individuals, the ICO must be notified within 72 hours. Procedures are in place to detect, report, and investigate a personal data breach. If a breach poses a high risk to individual rights and freedoms, the Council will notify those affected directly and without undue delay.

Employees, volunteers, and members must be careful not to use IT in any way that can be deemed unacceptable conduct; for example, discussing internal council matters on social media sites could result in reputational damage for the Council and individuals.

### **Privacy Notices**

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 2018 and the UK GDPR. The most common way to provide this information is in a privacy notice. This notice informs individuals about what the council does with their personal information. A privacy notice will contain the name and contact details of the data controller, the purpose for which the information is used, and the length of time for its use. It should be written clearly and advise the individual that they can withdraw their agreement for the use of this information at any time. Privacy notices will be accessible on the council's website and regularly updated to reflect any new data processing activities.

### **Information Audit**

The Council must undertake an information audit that details the personal data held, where it came from, the purpose for holding that information, and with whom the council will share that information. This includes information held electronically or as a hard copy. As part of its commitment to data security, the Council will ensure all data is securely stored and only retained as long as necessary for its specified purpose. The information audit will be reviewed at least annually or when the council undertakes a new activity. The audit review should be conducted ahead of the review of this policy, and the reviews should be minuted.

### **Individuals' Rights**

**UK GDPR** gives individuals rights with some enhancements to those rights already in place:

- the right to be informed

- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making, including profiling.

The enhancements of UK GDPR include the right to have personal data erased (the ‘right to be forgotten’) where data is no longer necessary and data portability at no cost. Any requests for data erasure will be handled promptly, with responses issued within a month. The Clerk has delegated authority from the Council to manage such requests.

### **Children**

There is special protection for the personal data of a child. The age when a child can give their consent is 13. If the council requires consent from young people under 13, it must obtain a parent or guardian’s consent to process personal data lawfully. Consent forms for children 13 and above will be written in age-appropriate language to ensure understanding.

### **Summary**

The main actions arising from this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council’s website. The policy will be considered a core policy for the Council.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices will be made accessible on the website and issued consistently.
- Data Protection will be included in the Council’s Risk Management Policy.

This policy document is written with current information and advice. It will be reviewed at least bi-annually or when further advice is issued by the ICO. All employees, volunteers and councillors are expected to always comply with this policy to protect privacy, confidentiality and the interests of the Council.

Date of last review: 16 January 2025

Date of next review: January 2027