EMERSONS GREEN
TOWN COUNCIL

Data Protection Policy

Date approved: 4th December 2025

Approved by: Finance and Partnership Committee

Next Review date: December 2028

Contents:

1.Introduction

We hold personal data about our employees, residents, suppliers, and other individuals for a variety of Council purposes.

This policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access in the course of their work.

In particular, this policy requires Officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Emersons Green Town Council will adopt procedures and manage responsibly all data it handles, respecting confidentiality and complying with contractual and legal obligations under data protection legislation.

The Council will periodically review and revise this policy in light of experience, comments from data subject, and guidance from the Information Commissioner's Office (ICO).

A review of this policy will take place in line with the schedule detailed above or in the event of a change in regulation.

2. Definitions

Business Purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, statutory, and legislative purposes, payroll, consultations, and business development purposes. Council purposes include the following: • Compliance with our legal, regulatory, and corporate governance obligations and good practice • Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests • Ensuring Council policies are adhered to (such as policies covering email and internet use)

	• Operational reasons, such as recording transactions, training, and quality control, ensuring the confidentiality of sensitive information, security vetting and checking • Investigating complaints • Checking references, ensuring safe working practices, monitoring, and managing staff access to systems and facilities and staff absences, administration, and assessments • Monitoring staff conduct, disciplinary matters • Promoting Council services • Improving services
Personal Data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts, members of the public, Council service users, residents, market traders, hirers, correspondents. Personal data we gather may include individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases, council records.
Sensitive Personal Data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

3. Scope

This policy applies to all councillors and staff, and volunteers who access, use or pass on personal data in their work. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

Our Data Protection Officer has overall responsibility for the day-to-day implementation of this policy, and any breaches may result in prosecution, reputational damage and loss of public trust.

Criminal offences include:

- Unauthorised obtaining, handling, or disclosure of personal data.
- Selling or offering unlawfully obtained personal data.
- Re-identifying de-identified personal data.
- Obstructing or altering data in response to subject access or portability.

4. Our Procedures

- **Fair and Lawful Processing**: We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

- **The Data Protection Officer's responsibilities**:
  - Keeping the Council updated about data protection responsibilities, risk and issues.
  - Reviewing all data protection procedures and policies on a regular basis.
  - Assisting with data protection training and advice for all staff members and those included in this policy.
  - Answering questions on data protection from staff, council members and other stakeholders.
  - Responding to individuals such as members of the public, service users and employees who wish to know which data is being held by Emersons Green Town Council.
  - Checking and approving with third parties that handle the council's data and any contracts or agreement regarding data processing.

- **Responsibilities of the IT Management Services:**
  - Ensure all systems, services, software and equipment meet acceptable security standards.
  - Checking and scanning security hardware and software regularly to ensure it is functioning properly.
  - Researching third party services, such as cloud services the company is considering using to store or process data.

- **The processing of all data must be**:
  - Necessary to deliver our services.
  - In our legitimate interests and not unduly prejudice the individual's privacy.
  - In most cases this provision will apply to routine business data processing activities.

  Our Terms of Business contains a Privacy Notice relating to data protection. The notice:
  - Sets out the purposes for which we hold personal data on customers, employees, residents and service users.
  - Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisors.
  - Provides that service users and correspondents have a right of access to the personal data that we hold about them.

- **Sensitive Personal Data:**
  In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

- **Accuracy and relevance:**
  We will ensure that any personal data we process is accurate, adequate, relevant, and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.
  Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Data Protection Officer.

- **Your personal data:**
  You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal

circumstances change, please inform the Data Protection Officer so that they can update your records.

- **Data Security:**
  You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Data Protection Officer will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

- **Storing data securely:**
  - In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it.
  - Printed data should be shredded when it is no longer needed.
  - Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
  - Data stored on CD's or memory sticks must be locked away securely when they are not being used.
  - The Data Protection Officer must approve any cloud used to store data.
  - Servers containing personal data must be kept in a secure location, away from general office space.
  - Data should be regularly backed up in line with the council's back up procedures.
  - Data should never be saved directly to mobile devices such as laptops, tablets or smartphones.
  - All servers containing sensitive data must be approved and protected by security software and strong firewall.

- **Data Retention:**
  We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

5. Subject Access Requests

Please note that under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them.

If you receive a subject access request, you should refer that request immediately to the Data Protection Officer, who may ask you to help us comply with those requests.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law.

- **Processing data in accordance with the individual's rights:**
  - You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Data Protection Officer about any such request.
  - Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.
  - Please contact the Data Protection Officer for advice on direct marketing before starting any new direct marketing activity.

- **Training:**
  - All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.
  - Training is provided through an in-house seminar on a regular basis.
  - It will cover:
    - The law relating to data protection.
    - Our data protection and related policies and procedures.
    - Completion of training is compulsory.

6. GDPR and Data Protection Act Provisions

Where not specified previously in this policy, the following provisions will be in effect on or before – May 2018

- **Privacy Notice – Transparency of data protection**:
  Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:
  - What information is being collected?
  - Who is collecting it?
  - How is it collected?
  - Why is it being collected?
  - How will it be used?
  - Who will it be shared with?
  - Identity and contact details of any data controllers
  - Retention period

- **Conditions for processing**:
  We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

- **Justification for personal data**:
  - We will process personal data in compliance with all six data protection principles.
  - We will document the additional justification for the processing of sensitive personal data and will ensure any biometric and genetic data is considered sensitive.

- **Consent**:
  The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

- **Criminal record checks:**
  Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

- **Data portability**:
  Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

- **Right to be forgotten**:
  A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

- **Privacy by design and default**:
  Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Data Protection Officer will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.
  When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

- **Data audit and register**:
  Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

- **Reporting breaches:**
  All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:
  - Investigate the failure and take remedial steps if necessary.
  - Maintain a register of compliance failures.

- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures.

Any breaches should be reported to our Data Protection Officer (Clerk to the Council) at clerk@emersonsgreen-tc.gov.uk

- **Monitoring:**
  Everyone must observe this policy. The Data Protection Officer has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

7. Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.
The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. A solicitor in breach of Data Protection responsibility under the law or the Code of Conduct may be struck off.
If you have any questions or concerns about anything in this policy, or wish to report a breach, do not hesitate to contact the Data Protection Officer (Clerk to Emersons Green Town Council) at clerk@emersonsgreen-tc.gov.uk or 0117 302 6989.

8. Responsibilities

Town Clerk:

The Town Clerk reports to Council and is responsible for:
- Ensuring GDPR objectives are achieved.
- Advising the Council and maintaining records of processing activities.
- Managing policies, procedures, and documentation.
- Arranging training for Councillors and staff.
- Reviewing compliance programmes and reporting findings.
- Ensuring contracts with service providers include GDPR/DPA compliance requirements.

Councillors and Staff:

All Councillors, staff, and volunteers must comply with GDPR, DPA, and related legislation when handling personal data.

9. Breaches of Policy

Disciplinary action, including dismissal, may be taken against any member of staff who contravenes this policy.
The Town Clerk, in consultation with the Chair of the Council, has authority to take immediate steps as necessary.

10. Links to Other Policies

This policy is linked to:
- Privacy Notice
- Publication Scheme
- Document Retention and Disposal Policy

11. Guidance and Additional Information

For guidance and enquiries relating to this policy, contact the Town Clerk, who is responsible for managing Data Protection compliance.
Further guidance is available from the Information Commissioner's Office (ICO):
- Website: www.ico.org.uk
- Telephone: 0303 123 1113
- Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF