GREAT BURSTEAD AND SOUTH GREEN VILLAGE COUNCIL

# Data Protection Policy

Adopted: March 2026

Next review March 2027

Great Burstead and South Green Council is fully committed to compliance with the requirements of Data Protection legislation. The Village Council follows the Data Protection Act 2018 and the General Data Protection Regulations. The Council will therefore follow procedures that aim to ensure that all employees, elected or co-opted members, contractors, agents, consultants, partners or other servants of the Council who have access to any personal data held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under this legislation.

**Introduction**

We hold personal data about our employees, residents, suppliers, volunteers 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.

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, social media and internet use);
- Operational reasons, such as 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, Councillors, volunteers, clients, suppliers and marketing contracts, members of the public, Council service users, residents, correspondents.

Personal data we gather may include:
Individual 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 and council records.

**Sensitive Data** Personal data about an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union affiliation, genetic data, biometric data, physical or mental health or condition, data concerning sex life or orientation criminal offences, or related proceedings – any use of sensitive personal data should be strictly controlled in accordance with this policy.

**Scope**
This policy applies to all Councillors, staff and volunteers. 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.

**Our procedures**
Fair and lawful processing.
We must process personal data fairly and lawfully in accordance with individual's 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 risks and issues;
- Reviewing all data protection procedures and policies on a regular basis;
- Assisting with data protection training and advice for all staff, Councillors, volunteers and those included in this policy;
- Answering questions on data protection from staff, Council members, volunteers 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 on them by Great Burstead and South Green Village Council;
- Checking and approving with third parties that handle the Council's data any contracts or agreement regarding data processing.

**Responsibilities of IT support**
- 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.

**Responsibilities of the Clerk**

- Acts as the Data Protection Officer as per the responsibilities above;
- Approving data protection statements attached to emails and other marketing companies;
- Addressing data protection queries from clients, target audiences or media outlets;
- Ensure all marketing initiatives adhere to data protection laws and the Council's Data Protection Policy.

**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 purpose for which we hold personal data on customers, employees, volunteers, residents and service users;
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers;
- 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 that 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). 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 purposes 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.

**Your personal data:**
Reasonable steps must be taken to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstance change, please inform the Clerk so that your records can be updated.

**Data security:**
Personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Clerk will establish what, if any, additional specific data security arrangements need to be

implemented in contracts with those third-party organisations.

**Storing personal data securely:**

- In cases when data is stored on printed paper, it will be kept in a secure place where unauthorised personnel cannot access it;
- Printed data will be shredded when it is no longer needed;
- Data stored on computers is protected by strong passwords that are changed regularly;
- Data stored on memory sticks will be locked away securely when they are not being used;
- Data will be regularly backed up in line with the Council's backup procedures;
- Data will not 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 the Council's retention policy.

**Subject access requests:**

Under the Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them.
If a subject access request is received, this will be referred to the Clerk.

**Processing information in accordance with an individual's rights:**

Any request by an individual not to use their personal data for direct marketing purposes will be abided by and the Clerk will be notified immediately.
Direct marketing material must not be sent by email unless there is an existing business relationship with them in relation to the services being marketed.
Great Burstead and South Green Village Council will only use data for the purpose of Council business.

**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 will be provided in-house when needed.

It will cover:

- The law relating to data protection;
- Our data protection and related policies and procedures.

Completion of training is compulsory.

**GDPR and Data Protection Act provisions;**

Where not specified previously in the policy, the following provisions will be in immediate effect.

**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 the Council.

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 rights or as part of a pattern of failures.