Greatham Parish Council

Information Security Policy

Adopted: 10th March 2021
Review due: March 2023

1. Purpose of Document

Greatham Parish Council recognises that information and the associated processes, systems and networks are assets and that the management of personal data has important implications for individuals. The Council believes that the security of information is essential.

This policy is to protect all information assets owned and used by Greatham Parish Council (GPC) and describes the Information Security Policies adopted by GPC. The objective of these policies is to ensure that appropriate standards of information security are maintained across the Council at all times so that:

- the public and all users of GPC's information systems are confident of the information used and produced.
- damage and interruption caused by security incidents are minimised.
- all legislative and regulatory requirements are met.
- the Council's equipment and facilities are used responsibly, securely and with integrity at all times.

This policy must also be read in conjunction with our Standing Orders and Code of Conduct. We are also guided by information provided by the ICO and our own Publication Scheme.

2. Version

This is version 1.0 of this policy, dated 10th March 2021

3. Overall Approach

It is not possible to set out precautions and actions to cope with all circumstances and conditions, therefore anyone handling sensitive and confidential information MUST take personal responsibility and make considered judgements in terms of how they handle this information whilst executing the business of GPC.

If in any doubt individuals should seek clarification from the Parish Clerk . Overall impact is determined by the degree of sensitivity of the information and the quantity involved, but you must remember that a single record about an individual can have a potentially significant impact on that individual if accidentally disclosed to others.

An easy sense check on whether information is sensitive or confidential is:

- Is the information covered by the Data Protection Act 1998 or any further duty of confidence?
- Could release of the information cause problems or damage to individuals, the public, the Council or a partner organisation? This could be personal, financial, reputation or legal damage.
- Is the information commercially sensitive, or could the originator reasonably have expected the information to be kept confidential?
- Could release of the information prejudice the outcome of negotiations or investigations?

If in doubt seek advice from the Parish Clerk and err on the side of caution, treating the information as sensitive and confidential, and in accordance with the "principle of least privilege" whereby individuals should not have access to any non-public information other than that required to carry out their role.

4. Definition

Information Security is defined as the preservation of:

- Confidentiality: protecting information from unauthorised access and disclosure;
- Integrity: safeguarding its accuracy and completeness; and
- Availability: ensuring that information is available to authorised users when required.

Information exists in many forms. It may be on paper, stored electronically, transmitted over a network, viewed in videos or films, or spoken in conversation. Whatever its form, or medium, appropriate protection is required to ensure business continuity and to avoid breaches of the law, statutory, regulatory or contractual obligations.

5. Privacy of Information

It should be noted that GPC is a public body and will seek to carry out its business in a public and transparent way. Much of its business is conducted in meetings open to the public. All information given at a public meeting of GPC is in the public domain, is likely to appear in the minutes and may be reported by the press. The Council publishes many of its documents on its website.

Additionally, the Council is subject to the Freedom of Information Act 2000 which provides public access to information held by public authorities. This means that GPC is obliged to publish certain information and its activities and members of the public are entitled to request information covered by the Act.

As a result, all information help by GPC may be made public through a number of formal processes including FOI requests, Data Protection requests, or the normal operation of GPC and the publishing of minutes.

However, councillors, staff and contractors should be aware that information should only be made public through these formal processes or in accordance with this policy. So, for example, just because information may be the subject of an FOI request at some point in the future, does not give license to distribute that information outside of the formal process. The formal processes exist to provide transparency and an audit trail of information flow.

Although the Council owns some IT equipment, this is limited, and much business (principally by email) is conducted on councillors' personal devices.

6. Protection of Personal Information

The Council may hold and use information related to employees, councillors, members of the public, and other data subjects for essential administrative and business purposes. When handling such information, the Council, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998. As such, this document should be read in conjunction with the Greatham Parish Council Data Protection Policy.

7. Responsibility for Information Security

Information security is the responsibility of all councillors, employees (temporary or permanent), contractors, agents, and anyone else processing information on our behalf. Every person handling information or using Council equipment is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the Council.

Staff and Councillors should have no expectation of privacy in their use of any GPC business system. Any correspondence, documents, records, or handwritten notes may be disclosable to the public, under the Freedom of Information Act 2000 or the Data Protection legislation. Any comments recorded or notes written must therefore be appropriate.

8. Data Classification

Data within GPC has different sensitivity levels. By classifying content according to sensitivity, a clear, meaningful value can be properly applied to data or sets of data to ensure appropriate protection and handling. This Policy defines four different data classifications and the process to ensure that the classifications are consistently applied by all councillors, staff, and other relevant individuals.

Failure to apply the correct Data Classification or failure to handle the data in the appropriate manner may result in accidental or deliberate loss or compromise of data.

Note: All information given at a public meeting of GPC is in the public domain and therefore becomes PUBLIC, regardless of its prior classification. Additionally, the Freedom of Information Act covers all recorded information held by a public authority. It is not limited to official documents and covers draft documents, emails, notes, recordings of meetings and telephone conversations, and the Data Protection Act covers personal data held by GPC.

However, outside of the formal processes and publishing timings, information should only be shared in accordance with the table below and as outlined in section 5.

Classification	Type	Application
PRIVATE Information which if lost or wrongly disclosed could cause very serious damage to the interests of GPC our councillors, staff and business partners.	PII - GDPR Sensitive, such as Racial origin, political opinion, religious belief,. HR – staff appraisals, contracts of employment, and Salary information. Commercially sensitive tender information.	Folders and documents should be set up to ensure only a specified authorised list of people are able to access them. Extract to physical media such as USB, DVD, CD etc. is not permitted without explicit authorisation and logging of such activities. Only authorised recipients to receive data via email. All physical media is encrypted. Access to the folder or document should be auditable by the author and system administrator. Do not print this data unless there is a critical need. Do not copy the document or data without authorisation from the data owner.
CONFIDENTIAL Personal information that can be traced to individuals, which if lost or incorrectly disclosed could cause distress, or damage the interests of GPC.	PII - GDPR personal data, such as name and address, email, telephone number, age, date of birth. Project plans, Budget data, Grant allocations prior to publication. Non-public information,	Folders and documents should be set up to ensure only a specified authorised list of people are able to access them. Extract to physical media such as USB, DVD, CD etc. is not permitted without explicit authorisation and logging of such activities. Only authorised recipients to receive data via email. All physical media is encrypted.

	communicated “in confidence” to GPC Councillors, staff or working party members by local authority, planning authority, enforcement, other councillors, or representatives of other bodies.	Access to the folder or document should be auditable by the author and system administrator. Do not print this data unless there is a critical need. Do not copy the document or data without authorisation from the data owner.
RESTRICTED No information that can be traced back to individuals but information which if lost or wrongly disclosed may cause limited negative effects for GPC.	PII – none Draft Internal policies Discussion documents for GPC meetings that represent the opinions of individual councillors.	Folders and documents should be set up to ensure that they cannot be accessed by unauthorised parties. Extract to physical media such as USB, DVD, CD etc. is not permitted without explicit authorisation and logging of such activities. Only authorised recipients to receive data via email. All physical media is encrypted. Access to the folder or document should be auditable by the author and system administrator.
PUBLIC No personal or other sensitive data held.	PII – none Minutes, financial statements and documents that have been discussed in GPC meetings. Newsletters, flyers, website and forum postings.	Folders and documents should be set up to ensure that public data can be easily identified. Extract to physical media such as USB, DVD, CD etc. is permitted. Any recipients may receive data via email. Access to the folder or document should be auditable by the author and system administrator.

9. Compliance with Legal and Contractual Requirements

9.1 Use of GPC equipment

Where GPC IT equipment is provided it must only be used for authorised purposes. Limited personal use is permitted.

9.2 Use of Personal equipment

Councillors and staff conducting Council business on their own personal equipment have a responsibility to follow established Good Practice to protect against malicious software and unauthorised external access to networks and

systems. Information should be regularly backed up. GPC software should not be copied without authority, nor should copies of GPC information be made for personal use.

9.3 Security and encryption

For either GPC or personal equipment used for GPC business the following applies.

Firewalls must be used where available. For Windows 10 devices Defender must be used, and for all devices with Windows operating systems earlier than Windows 10, effective antivirus software must be installed and used, see below.

Unless permanently stored in a dwelling that is locked when not in use (eg a councillor's or officer's home), all devices used to store council files and/or emails must as a minimum have this data encrypted:

- Android devices:
    - Those running v4.4 or above are automatically encrypted.
    - Those running below v4.4 must not be used for council data unless they are shown to be encrypted.
- Apple devices:
    - Encryption is standard in all versions.
    - For Mac devices File Vault disk encryption must be turned on as detailed in the Appendix to this document.
- Windows devices
    - Devices running Windows XP or below must not be used for GPC data
    - Devices running versions of Windows with BitLocker available (eg Windows 8 or 10 Pro and Enterprise) must be encrypted using BitLocker
    - Devices running versions of Windows without BitLocker must use VeraCrypt or similar third party package to encrypt ideally the whole device but as a minimum all council files and emails.

If in any doubt, councillors and officers must ask the clerk for advice.

9.3 Removing council data from devices

When a councillor ceases to be a member or an officer ceases to be employed, they must remove all council data from all their personal devices. Similarly, when a councillor or officer no longer uses a specific device for council business, all council data on that device must be removed.

The Clerk will immediately stop access to the Council's email system on receipt of a councillor's resignation or when they cease to be elected.

Data removal must be by either:

- physical destruction of the data storage
- or wiping with a suitable utility (ask the clerk for recommendation of a suitable utility at the time the device is changed).

In addition, council data must be permanently deleted on any associated cloud storage. If required by the council or the clerk, the councillor or officer must sign a statement that all data has been removed.

10. Email (internal or external use)

The following policy applies to the use of email:

- All Staff and Councillors will be issued a Council email account which must be used when transacting on behalf of GPC. They must not use non-GPC email accounts to conduct or support GPC business.
- In the event that Councillors or staff are sent emails to their private email accounts that pertain to GPC business, they should forward that mail to their GPC account and only enter into correspondence via GPC accounts.
- Mail must not be forwarded from GPC accounts to another private account.
- Any information held in personal email accounts (such as Gmail, Hotmail etc) may be subject to Freedom of Information if it relates to the official business of the public authority. All such information which is held by someone who has a direct, formal connect with the public authority is potentially subject to FOI regardless of whether it is held in an official or a private email account.
- Internet email is not a secure medium of communication; it can be intercepted and read. Do not use it to say anything you would not wish to be made public. If you are sending confidential information by email this should be sent using password protected attachments.
- Email should be treated as any other documentation. If you would normally retain a certain document in hard copy you should retain the email.
- Do not forward email messages unless the original sender is aware that the message may be forwarded. If you would not have forwarded a copy of a paper memo with the same information do not forward the email.
- Your email inbox should be checked on a regular basis.
- If you receive an email from a suspicious source or with an odd or unexpected subject title, you should treat it with suspicion and, if unsure how to proceed, refer to the Clerk in the first instance.
- All official external e-mail should carry the official Council disclaimer, and Automatic forwarding of email is not permitted to prevent confidential material being forwarded inappropriately.
- As with many other records, email may be subject to discovery in litigation. Like all communications, you should not say anything that might appear inappropriate or that might be misinterpreted by a reader.
- Viewing, displaying, storing (including data held in RAM or cache) or disseminating materials (including text and images) that could be considered to be obscene, racist, sexist, or otherwise offensive may constitute harassment and such use of the Facilities is strictly prohibited. The legal focus in a harassment case is the impact of the allegedly harassing material on the person viewing it, not how the material is viewed by the person sending or displaying it.
- Councillors will be required to surrender their email account and all of its contents to the Clerk at the end of their term of office or if they decide to leave the Council.

11. Social Media and Online Participation

This policy includes Social Media and Online Participation, i.e. forums, blogs, websites and so on. Members and staff should not disclose personal information about GPC's staff, members or business online, unless expressly authorised to do so.

Members using social media should always be aware of their association with the Council, be aware that they cannot speak on behalf of GPC and ensure that their posting is consistent with this. Councillors are personally responsible and liable for the content they publish. They should be mindful that posts might remain public indefinitely.

12. Information Disposal

All members and staff have a responsibility to consider security when disposing of information in whatever medium and format it is kept.

13. Monitoring Policy

The Clerk on behalf of GPC may monitor individual's actions with regard to Information Security. Whilst GPC recognises the importance of an individual's privacy it needs to balance this against the requirement to protect others and preserve the integrity and functionality of GPC. The Principal reasons for this are to:

- detect any harassment or inappropriate behaviour by councillors or employees, ensuring compliance with contracts of employment and relevant policies including the health and safety, ethical and sex discrimination policies.
- ensure compliance with this policy.
- detect and enforce the integrity of GPC's environment and any sensitive or confidential information belonging to or under the control of GPC.
- ensure compliance by users of the Facilities with all applicable laws (including data protection), regulations and guidelines published and in force from time to time; and • monitor and protect the wellbeing of employees.

Where staff or councillors are using their personal equipment, GPC will respect the privacy of users' own files. However, GPC must reserve the right to examine systems, directories, files and their contents, on personal equipment e.g. laptops, iPads and mobile phones to ensure compliance with this policy and the legal and statutory regulations. Where a Freedom of Information request is received by GPC, the Clerk has the right to access all data held by a member relating to Council business.

. Access shall be limited to the least action necessary to resolve the situation and/or provide the information requested

14. Breaches and Reporting

Where Council members, employees or service delivery partners have acted in accordance with this standard, but a breach occurs through the action of others, they will be deemed to have acted reasonably. However, if Council members, employees or service delivery partners are found to be in breach of the policy and its guidance then they may be subject to disciplinary or other appropriate action.

All staff and members should report immediately to the Clerk, or to the Chair:

- any observed or suspected security incidents where a breach of the GPC's Information Security Policy has occurred.
- any security weaknesses in, or threats to, systems or services; and
- any Software malfunctions.