



GILLINGHAM TOWN COUNCIL
The Town Hall, School Road, Gillingham, Dorset SP8 4QR

Information Security Policy

1. Introduction

Gillingham Town Council issues this policy to meet the requirements incumbent upon them under UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 for the handling of personal data in the role of controller.

Gillingham Town Council processes large amounts of personal data, special categories of personal data and confidential data and has a responsibility to maintain privacy and security regarding this information. To this end, the **confidentiality, integrity, availability** of this information needs to be protected from harm in a way that is proportionate to the risks to the information.

The purpose of this policy is:

- To protect the information held by Gillingham Town Council and its reputation
- To enable secure information sharing to deliver services
- To complement and safeguard information enabling business growth
- To protect the organisation from legal liability and inappropriate use
- To encourage consistent and professional use of information and systems
- To ensure everyone is clear about their roles in using and protecting information
- To maintain awareness of information security
- To protect the organisation's employees

2. Scope

This policy applies to all employees of Gillingham Town Council including councillors, contract, agency and temporary staff, volunteers and employees of partner organisations working for Gillingham Town Council ,whenever and wherever that they process the organisation's information.

The policy applies to all forms of information including, but not limited to, text, pictures, photographs, maps, diagrams, video, audio, CCTV and music, which is owned by, administered or controlled Gillingham Town Council, including information, which is:

- Spoken face to face, communicated by fixed line, by mobile telephone, or by two-way radio
- Written on paper or printed out from a computer system. This may include working both on-site or remotely (e.g. at home)
- Stored in structured manual filing systems
- Transmitted by email, over the Internet, fax (if in place) and via wireless technology
- Stored and processed via computers, computer networks or mobile computing devices including, but not restricted to, PCs, mobile phones, laptops, tablet PCs, electronic organisers and personal digital assistants (PDAs).
- Stored on **any** type of removable computer media including, but not restricted to, CDs, DVDs, tapes, microfiche, diskettes, USB memory sticks, external hard disks, and memory stores in devices including, but not restricted to, digital cameras, MP3 and MP4 players.

3. Legal Principles

In execution of this policy, Gillingham Town Council will comply with the data protection principles of the UK GDPR and the Data Protection Act 2018. Specifically, the principle that personal data is *processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.*

Gillingham Town Council will adopt the appropriate technological and organisational measures to ensure compliance with the Data Protection Principles by carrying out the necessary procedures.

4. Roles and Responsibilities

All users which include staff, councillors, contractors, consultants, suppliers and volunteers must:

- a) Be familiar with this policy and other relevant policies and procedures including, but not limited to:
 - i. Data Protection Policy
 - ii. Data Breach Policy
 - iii. Data Retention Policy
 - iv. Dorset Council Acceptable Usage Policy
- b) Play an active role in protecting information in their work
- c) Read and act on any training and awareness, and communications regarding information security and ask for clarification if these are not understood

- d) Take care when handling information to ensure it is not disclosed to those without the need to know or are not approved
- e) Report any breaches, near misses, or incidents to the organisation via the organisation's Data Breach Policy and procedures

Gillingham Town Council is required to:

- a) Appoint a Data Protection Officer
- b) Approve this policy
- c) Actively promote a culture of privacy and security
- d) Ensure security and privacy is considered throughout the development of any new service, process or project
- e) Cascade any relevant communications regarding information security
- f) Ensure Information Asset Owners and Information Asset Custodians are assigned for its critical information assets

Ultimately Gillingham Town Council is accountable for its information, therefore there may be other elements that this cohort deliver as part of their roles.

Information owners are required to:

- a) Update the organisation's Record of Processing Activities (Information Audit / Inventory) at least on an annual basis
- b) Contribute to the risk assessment on their information assets, and own the risks, the potential mitigations, and the implementation of any controls
- c) Ensure Business Continuity Plans are in place for their information assets as well as being exercised / tested
- d) Be involved in any investigation regarding breaches, incidents or near-misses associated with their information assets

Dorset Council ICT is required to:

- a) Be the custodian of electronic systems which process information assets
- b) Assist information owners and the Data Protection Officer in identifying any risks associated with the processing of information on the organisation's electronic systems
- c) Assist from a technical level with any investigation regarding breaches, incidents or near-misses associated with the organisation's information assets
- d) Report any unauthorised access, or unauthorised access attempts to information systems
- e) Ensure software and operating systems are appropriately licensed

Data Protection Officer is required to:

- a) Monitor compliance with Data Protection Law and this policy, reporting this to the Full Council of Gillingham Town Council
- b) Assist the organisation with any Data Protection Impact Assessment which could include identifying risks and recommending controls to mitigate those risks where practicable.
- c) Assist the organisation with any queries they have regarding data protection

The contact details of the Data Protection Officer may be found in Section 15.

5. Data Protection by Design

It is a statutory requirement that any activity involving a high risk to the data protection rights of the individual when processing personal data be assessed by the Data Protection Impact Assessment. Prior to the assumption of any such activity i-west must be consulted and an initial screening be conducted assessing risk.

The concept of *data protection by design* will be a guiding principle in achieving the security of individual's data protection rights. The following will be considered as part of data protection by design

- **Encryption** – the use of strong cryptography to protect data at rest and in transit
- **Pseudonymisation** – the use of a unique reference number
- **Data Minimisation** – information is only personalised or personally identifiable for the minimum amount of time and only until the purpose is achieved
- **Technical Measures** – The Town Council's IT Provider, Dorset Council is responsible for ensuring that its infrastructure / network is as safe and secure as is reasonably possible

6. Data Security and Storage of Records

The Town Council will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records that contain personal data will be secured when not in use.
- Papers or documents containing special category personal data must not be left on office desks, pinned to notice/display boards*, or left anywhere else where there is general access (please refer to the Special Category of Personal Data Policy for additional information on protecting this data).

**An exception to this could be allergy information where the risk of staff being unaware of certain medical conditions outweighs the information risk. However,*

the Town Council will still consider measures to reduce the risk of those without the need to know from viewing this information.

- Personal data must only be stored and accessed on the Town Council network.
- Access to Town Council computer files is restricted to authorised users who have password access in place. Staff and Councillors are reminded to have strong passwords and to change them if they have, or there is a risk that they have, been compromised.
- Encryption is used to protect all portable devices and removable media, such as laptops, which hold personal data.
- Staff and Councillors are required to sign and adhere to the Town Council's ICT Acceptable Use Agreement.
- The Town Council has clear procedures for the automatic backing up, accessing and restoring of personal data held on Town Council systems.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.
- The Town Council ensures that its IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users are assigned a clearance that determines which particular files are accessible to them. Members of staff are not, as a matter of course, granted access to the whole management information system (SIMs). Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

7. Bring Your Own Device (BYOD)

Staff Owned Devices

- Staff must not use their own devices to take images of young people.
- Only Town Council equipment may be used and images must be deleted as soon as they are no longer required, saved securely on the Town Council system and deleted in accordance with the retention policy.
- Pass-codes or PINs must be set on personal devices to aid security and, where possible, encryption applied to the device.
- Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements.
- Users must log out of Town Council programmes and applications when they are not in use.
- The device must have the latest updates applied.
- Passwords must not be saved, for example to the browser history.
- Users must not download data locally to the device (e.g. email attachments).

8. Remote Access

- Access to Town Council systems should be via secure portal using a VPN.
- If secure remote access is not possible, users must only remove or copy Town Council or sensitive data from Town Council premises if the storage media, portable or mobile device is encrypted, and password protected.
- Documents must not be saved locally to the user's personal device for example to the hard drive, desktop or personal USB stick.
- The data must be securely deleted from the USB stick once it has been transferred or its use is complete.

9. Secure Transfer of Data and Access Out of Town Council

The Town Council recognises that personal data may be accessed by users outside of the Town Council or transferred to authorised third parties. In these circumstances:

- Data should be transferred according to its sensitivity, Special Category Data, financial, or high volumes of data may only be transferred via secure, encrypted means for example via secure email or a secure SharePoint when permission has been given.
- Transferring the data must be in accordance with Town Council business and not for personal use.
- If information is to be hand delivered then an index of what is included, and a signed receipt must be included and retained by both parties.
- Users must be clear of the legal basis upon which they are sharing the information with any third party. Please refer to the Data Protection Policy for the grounds for processing. In the event of any queries, advice from the Data Protection Officer (see Section 15) must be sought.
- For larger data transfers, such as moving a new data system or data processor, the Town Council must ensure that there are adequate safeguards in place with the 3rd party to ensure the security of the information which is transferred and compliance with data protection laws. This should be defined in a Data Transfer Agreement.
- Particular care should be taken if it is intended that data be transferred to or from another Country (for example the location of the server is based outside the UK), particularly outside Europe (restricted transfer). Advice should be taken from the DPO in advance to consider whether appropriate safeguards are in place.

Please refer to [Appendix 3](#) for guidance around secure email, and [Appendix 2](#) for guidance on setting up an email delay.

10. Digital images including photographs and videos

As part of our Town Council activities, the Town Council may take photographs and record images of individuals, including to:

- Identify individuals, for example to identify staff and Councillors to access the Town Council, for medical conditions or dietary needs.
- Promote the town.
- Celebrate achievement in displays around the Town.

The Town Council will obtain written consent for photographs and images to be used in the wider public domain, such as:

- On display in Town Council buildings.
- On the Town Council website.
- On promotional materials or literature.
- On Town Council social media sites.
- In local media, e.g. to celebrate achievement, promote Town Council activities.

Consent can be refused or withdrawn at any time. The Town Council must ensure that an adequate system is in place to permit the withdrawal of consent. However, once images have been posted to the internet including social media, the Town Council has no control over the images being reposted to others, this must be made clear in any privacy notice, or transparency information provided to the data subject.

When using photographs and images in this way the Town Council will not accompany them with any other personal information about the individual, to reduce the risk of them being identified, unless this is with the specific consent. Please refer to our Image Consent Form.

11. Filming and Photography at Town Council Events

The Town Council does not generally permit filming by any adult, other than Town Council employees or approved contractors, using video equipment, mobile phones, or any other device on Town Council property; however still photography is allowed. Events should be considered individually regarding whether filming and/or photography should be permitted.

If parents wish to take photographs of their child at a Town Council event they should abide by any directions given, only take appropriate images, be sensitive to other people and try not to disrupt or interrupt concerts, performances or events. Photographs taken purely for personal use are exempt from the data protection act; however, these photographs must not be used in the public domain, including social network sites such as Facebook, without the prior permission of the Town Council and the parents of all children featured in the photographs.

12. Security Incidents and Breaches

Wherever it is believed that a security incident has occurred or a 'near miss' has occurred, the organisation and the Data Protection Officer must be informed immediately and the Security Incident Management (SIM) process must be carried out. The SIM is designed to manage, investigate, report and provide 'Learning from Experience' (LFE) to avoid future incidents occurring.

In any case an incident must be reported no later than 24 hours from identification, except where a malicious incident has occurred. The learning culture within the organisation seeks the avoidance of a blame culture and is key to allowing individuals the confidence to report genuine mistakes.

Further details on security incidents and data breaches can be found in the Data Breach Policy.

13. Monitoring and Discipline

Compliance with this policy shall be monitored through a review process. This will be agreed with the Data Protection Officer, and compliance will be reported to Full Council.

Should it be found that this policy has not been complied with, or if an intentional breach of the policy has taken place, Gillingham Town Council, in consultation with The Town Clerk, shall have full authority to take the immediate steps considered necessary, including disciplinary action.

14. Review

This Information Security Policy was presented to Finance and Policy Committee on 18th September 2023 for approval, minute no. 588g and ratified at Full Council on 25th September 2023.

Future reviews will be done either annually or when there are changes to current legislation, DPO or Town Clerk, whichever is the sooner.


Signed:

Date:

Mayor of Gillingham

Appendix 1 – Information Security Procedures

All consumers must protect personal data at rest by applying appropriate security:

- 1) **Locking screens** when away from their desks (using  +L)
- 2) By **disposing of information and equipment** in an appropriate manner:
 - a. Equipment – via the organisation’s accredited provider
 - b. Paper – using either a cross cut shredder or the organisation’s accredited provider which may be facilitated by Confidential Waste receptacles.
- 3) Ensuring **special categories of personal data**¹ is given extra security, and at a minimum is locked away when not in use (¹ *race/ethnicity, religion, genetics, health, photos, sexual orientation, trade union, political opinions*)
- 4) Using encryption when **processing personal data offsite** e.g. working at home (either on an encrypted device or an encrypted USB stick owned by the organisation). For encrypted sticks users must
 - a. ensure the information is uploaded back to the organisation’s network as soon as possible, and;
 - b. only process the data on the stick and not process or save the data outside of the stick (e.g. locally to the device).
- 5) When processing data on an unmanaged (**personal device**) users must ensure:
 - a. The device is protected by PIN, Password or fingerprint, and ideally encrypted
 - b. That the organisation’s systems (e.g. Webmail) are not left logged in, or the save password function used
 - c. That files (e.g. attachments) are not downloaded locally to the device, unless in an emergency where measures are to be taken to delete the information after use
- 6) **Data taken offsite must be protected at all times**, as well as the above, users must:
 - a. Keep information and equipment on their person at all times (e.g. when stopping off on the way home)
 - b. Be held in an appropriate receptacle (e.g. bag) to reduce the risk of opportunistic theft
 - c. Not store leave the information and equipment in a vehicle when not in use
 - d. Consider whether data minimisation could be used. For example:

- i. Not making the information personally identifiable, by using pseudonymisation (e.g. Unique reference or initials)
- ii. Using a code system or colour code system to identify key indicators (e.g. allergies)
- iii. Not having the organisation logo on any hardcopy documents
- iv. Using encryption to protect the data (e.g. encrypted device rather than hard copies)

7) **Ensuring care is taken with emails**, by applying the following:

- a. Was I expecting this email?
- b. Does it look and feel right?
- c. Can I check (by other trusted means) that the email is legitimate?
- d. Not clicking any links or opening any attachment with validating them
- e. Using blind copy (BCC) when emailing more than one external user
- f. Double checking the email address when sending emails
- g. Encrypting personal data to external addresses ([See Appendix 3](#))
- h. A one minute email delay rule is in place on all emails sent, this provides a safety net where all emails sent are held in Outbox for one minute before delivery allowing the user to edit/delete ([See Appendix 2](#))

8) Ensuring any **information disclosed verbally** is

- a. Validated – the person calling/present is known to have the need to know
- b. Documented – a summary of what was disclosed and filed

9) Ensuring any **information sent via post has the address double checked** – where possible copy and paste from a system, is marked *Private & Confidential*, and sent via recorded or special post for special categories of personal data.

Appendix 2 – Setting up an email delay (in Outlook 2013)

This can either be setup by a user or, with the aid of the organisation's IT Team, can be setup corporately.

1. Click the **File** tab.
2. Click **Manage Rules and Alerts**.
3. Click **New Rule**.
4. In the **Step 1: Select a template** box, under **Start from a Blank Rule**, click **Apply rule on messages I send**, and then click **Next**.
5. In the **Step 1: Select condition(s)** list, click **Next**.
If you do not select any check boxes, a confirmation dialog box appears. If you click **Yes**, the rule that you are creating is applied to all messages that you send.
6. In the **Step 1: Select action(s)** list, select the **defer delivery by a number of minutes** check box.
7. In the **Step 2: Edit the rule description (click an underlined value)** box, click the underlined phrase **a number of** and enter the number of minutes for which you want the messages to be held before sending.
Delivery can be delayed up to 120 minutes. I would suggest 1 or 2 minutes.
8. Click **OK**, and then click **Next**.
9. Select the check boxes for any exceptions that you want.
10. Click **Next**.
11. In the **Step 1: Specify a name for this rule** box, type a name for the rule.
12. Select the **Turn on this rule** check box.
13. Click **Finish**.

After you click **Send**, each message remains in the **Outbox** folder for the time that you specified.

Appendix 3 – Securing an email in transit

The three main risks associated with email are:

1. Emails are intercepted in transit
2. Emails are sent to the wrong recipient
3. Email addresses are disclosed to those without the need to know

This process covers risk 1 and enables the secure exchange of information over email (in the absence of a secure email portal).

1. Document the information in an MS Office document
2. Ensure that this is not the source/primary document – if it is then create a copy
 - i. Do not encrypt the source document – if you do, and forget the password you are unlikely to be able to gain access to the information again!*
3. Have the document open, and then click
 - a. File
 - b. Protect Document
 - c. Encrypt with Password
 - d. Create a strong password (minimum of 8 characters) – you could use a password generator <https://passwordsgenerator.net/> or pre-agree one with the recipient
 - e. Apply this password to the document
 - f. Save
4. Attach the secured document to an email and send it to the recipient
5. Communicate the password by other trusted means e.g. Phone call, or message. Before telling them the password ensure you:
 - a. Are communicating with the correct person; and
 - b. Confirm that they have received the email

It should be noted that encrypted attachments are sometimes blocked by email gateways as they cannot inspect the contents