Information Protection and Handling Standards

Our customers need to know that we can be trusted custodians of their information. We also have a responsibility under the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA) to process personal data in a manner that ensures appropriate security of the data. Each of us is responsible for protecting the information we collect and is in our care, identifying and managing risk, from talking to customers to sharing any amounts of information.

What is information?

Information is data that is both collected/created and presented within a context that gives it meaning and relevance, leading to an increase in understanding. This includes personal data – any information relating to an identified or identifiable living individual.

These Standards cover information in the council's care. It includes information about our customers, as well as other information used in running our business – for example, management or personnel records, policy papers, staff instructions, contracts, tender submissions. The term 'sensitive information' is used throughout these standards to encompass all data of this nature.

Information will be held or moved in a number of ways: on paper (including notepads and post-it notes); CD or DVD; by email; by telephone or video conference; in Council computer systems.

Key means of protecting and handling information are actions based upon the 6 principles that apply to all personal data:

- Processing [i.e., collecting, storing, using, handling, disposing] is lawful, fair and transparent;
- Creation/collection and use is only for specific, explicit, lawful processes;
- Processing that ensures adequate but not excessive information and/or personal data;
- Procedures are in place to maintain accuracy;
- Retention of information and data is only for as long as required by business need and/or law and appropriate disposal procedures are in place;
- Appropriate technological and organisational security measures are in place.

1.0 Capturing Information

1.1 Environment

- Be aware of your surroundings when capturing information.

- If you are having a conversation with a service user or colleague that includes gathering and discussing personal and/or special category (sensitive) information, ensure you are in a private area, to mitigate the risk of others being able to watch and/or overhear.

- Don't discuss council business issues or information about service users with colleagues in public places, such as on the train.

- In the same way, be aware of anyone who may be able to see information you are writing on paper or typing on a screen. Assess what action you can take to protect personal and sensitive information, e.g. turning your screen so that only you can see what you're capturing.

1.2 Data Minimisation

- Only capture the information you **need** to carry out a specific activity. To do this, make sure you know what you need. Capturing more information than necessary makes managing that information more difficult; can obscure relevant data; and complicate decision-making processes. It is also in breach of the Data Protection Act 2018.

1.3 Centralisation

- If you are capturing information on paper and/or on an electronic device (such as your encrypted laptop) on an ad hoc basis, ensure you save this information to an appropriate place in a relevant central system (e.g., Liquid logic; team shared drive or filing system) as soon as possible, no longer than 3 working days after the event and preferably on the same day. Once saved to the system, destroy the original copies, which are now duplicates.

- Please note: where duplicate records are required for business continuity reasons, processes need to be in place to ensure they are appropriately protected, accessible and kept up to date.

2.0 Access to Information

Access to information must always be restricted only to those who have a legitimate business need to access it.

Access controls should reflect the sensitivity of the information, with tighter controls for more sensitive information.

2.1 Council Buildings

- Protect information by safeguarding against unauthorised entry to council buildings and offices. Staff are expected to wear their official Gloucestershire County Council identity badge on Council premises and when on official business out of the office.
- Challenge anyone without an ID badge. If you are in doubt as to whether someone is a member of staff, challenge. If necessary, report to Custodians or Main Reception and your manager.
- Ensure visitors sign in and accompany them through the building.
- Ensure contractors are issued badges with access appropriate to the work they are carrying out. They must return their badges at the end of each day.

2.2 In the Office

- Adhere to the Clear Office Policy: **don't** leave personal and/or sensitive information on your desk **whenever** you are not around. This includes overnight. All information **must** be locked away securely to restrict access.
- Lock your computer when your leave your desk (using Ctrl + Alt + Delete keys and select lock computer or using  + L keys).
- Choose a password carefully, making sure to read the password guidance on how to keep it strong. Never share your, or use someone else's, login details and password. Ensure you comply with the GCC password policy.

- Store paper documents containing personal or sensitive information in a locked room, cabinet or container. Remember; don't leave keys to lockable storage in a place where they can be accessed easily. Keep them in a secure key safe.

- Never access information unless it is part of your job, and you have a business need to do so. Operate on a "need to know", not a "nice to know" basis. Ensure the systems you work with apply role-based access and maintain adequate audit trails.

- Keep printers and photocopiers clean. Stay with the machine until it completes printing personal or sensitive information before returning to your desk. Ensure you collect all your material and take it with you.

2.3 Out of the Office

- Read and follow the Guidance on Handling and Securing Paper Records Out of the Office. Always ask yourself the question, 'Do I really need to take this information out of the office?' The best way to protect information is to leave it safely on council premises.

- Never leave personal or sensitive documents in your vehicle. In very exceptional circumstances where you have no alternative, ensure that they are in the boot, out of sight and that the vehicle is locked. Remember you must use sound judgement and be able to account for your actions.

- Don't allow family members, friends, or visitors to use the council's portable devices (e.g., laptops) or to access council information.

- If you must store information outside of the office, then consider the safest place to do so. Do not store your electronics and paper files together, as thieves will often target electronics and valuables; while laptops are encrypted notebooks are not.

- Anti-virus software and security patches are in place to protect the council's computers and are frequently and automatically updated. You must ensure your laptop is regularly connected to the network to keep the security up to date (at least once a week if you work predominantly remotely). You must not disable security settings; if you suspect a virus, contact the ICT Service Desk immediately.

- For additional protection, all software acquired for use on council computer equipment must be purchased through the ICT Service Desk. You must not install personal or unsolicited software onto a council machine. See the Software Management Policy for more details.

3.0 Transferring Information

Before transferring any information, **always** ask:

1. **Do you need to transfer this information – is it really required?** Always assess the risks of transferring information.
2. **If the transfer is necessary, do you need to send all of the information or are only parts of it required?** Only ever send what you absolutely need to and no more.
3. **Do you have the authority to transfer / release the information?** You must have permission from the appropriate manager or Information Asset Owner **before** taking any action. For routine transfer/release this can be achieved through approved procedures, rather than permission on a case-by-case basis. Bulk transfers of information require the appropriate Information Asset Owner's approval. The Information Assurance team can provide a list of current Information Asset Owners.
4. If you have the authority to send the information and are sure you need to send it, **have you made appropriately secure arrangements for the transfer**? If you are transferring personal, special category or sensitive data via email then you must use Egress.

3.1 Internal Post

- Always use a sealed, fully addressed envelope. Ensure that the envelope is addressed to an individual and includes their full name; job title; team; and location.
- If you are sending personal and/or sensitive information, hand deliver the information directly to the recipient.

3.2 External Post

- Avoid using external post where possible, as you have very little control over the terms and security measures for the transfer.
- Information can be sent by post or by the courier service, depending on the volume of information being transferred. Contact the General Office for more details on using these services.
- Double check that you have the correct destination and postal address for the information. Contact the recipient to confirm, if necessary. Always use a full address.
- Mark post containing personal and/or sensitive information as “Private & Personal”; “Confidential”; or “Addressee Only” to limit access. Consider double enveloping for increased security.
- Always use recorded delivery or a bonded courier if you are sending quantities of personal and/or sensitive information.
- If you are sending information to a PO box, contact the recipient to confirm the address and once sent, to confirm that they have collected the information.

3.3 Email

3.3.1 Sending information

- When sending personal and special category data and/or sensitive information by email:
    - Always double check the recipient you are sending to, even if it is an internal email address as some names are duplicated and may not be the person you are intending to email.
    - Take all possible steps to ensure that emails are sent only to intended, appropriate recipients.
    - Use Egress Switch (Secure Email) to encrypt emails and attachments containing personal or sensitive information that are being sent to external email addresses.
    - Some e-mails containing personal or sensitive information do not need to be encrypted – please check the exceptions list.

    - Where information is being exchanged with members of the public, ensure that Egress is used.

- Where appropriate consider putting a delay on your emails, from when you press send to the email actually being sent, as a good way to mitigate the risk of causing a breach.

- If you are sending information out to multiple external individuals, put email addresses in the “Bcc” field, rather than the “To” field, so that individuals can’t see each other’s names and addresses. This protects individuals’ personal data.

- However, you should only use Bcc when absolutely necessary. Be open about who you are copying – the council acts as a transparent and accountable organisation so Bcc should not be used to ‘hide from the data subject’ other colleagues you are legitimately copying in.

- Always adhere to the council’s Internet and Digital Communications Policy.

3.3.2 Receiving Information

- Don’t open attachments to an email unless you are sure about the identity and trustworthiness of the sender

- Be particularly wary of phishing emails. If you receive one, you should delete it immediately and follow the relevant phishing guidance.

- If you are a GCC staff member and you need a method for third party organisations to send you large files securely then Egress large file transfer is a suitable solution.

3.4 Telephone / Video Conferencing

- Never give out any personal and/or sensitive information over the phone unless you are absolutely sure who you are giving it to and that they are entitled to receive that information. If you are unsure who they are and they work in a professional capacity, offer to call them back through their organisation’s switchboard/reception.

- If you are in doubt and cannot prove the identity of the caller, **don’t** share information.

- **Don't** discuss information where it can be overheard, for example in public or on a mobile telephone in public.
- **Don't** leave personal or sensitive information on voicemail.

3.5 Texting / Instant Messaging

- Text messages can be used to maintain contact with service users and arrange/change appointments. It **must not** be used to transfer personal and/or sensitive data.
- Content of any text/instant messages should be uploaded to the relevant electronic record for that individual within 24 hours.

4.0 Storing Information

4.1 Paper Records

- Paper records should only be created if absolutely necessary. Electronic records are more secure than paper as GCC has implemented technological solutions such as encryption to protect electronic data on GCC devices.
- Paper documents containing personal and/or sensitive data **must** be stored in a suitable locked container (e.g., a filing cabinet or cupboard) or a locked room.
- Do not store information on your desk – only have it out on a desk when you are working on it.
- When working from home, avoid use of paper records as far as possible. If there is a genuine business need for using paper, ensure storage of paper records is as secure as if you were on GCC premises. A locked filing cabinet would be best, however if this is not possible then they must be stored safely, out of sight and away from other valuables (such as your laptop).
- Store semi-current paper records (records that are closed or you don't need on a daily basis but need to keep for legislative/business reasons) in the Records Centre. You will still be able to request and retrieve the

information stored there. Check the Corporate Retention Schedule to ensure that records are kept for the appropriate length of time.

- Transfer council records of permanent value to Gloucestershire Archives.

4.2 Electronic Records

4.2.1 Shared Networks (S: and G: drives)

- Ensure that the following information is saved to a relevant shared network directory (e.g., S: or G: drive):
    - Records evidencing business transactions and policy (e.g., reports, policy documents)
    - Gloucestershire County Council (GCC) information, that provides evidence of decision-making.
- Organise folders on shared networks according to the functions and activities of your service area/team, rather than the business structure. Structures change regularly but functions and activities remain the same over time.
- Save information in relevant folders and files with names that are meaningful and easily understandable to all members of staff.
- Name documents consistently and logically, avoiding abbreviations. Follow the GCC naming conventions.
- Only save one copy of the information, deleting duplicates, notes, and drafts that have been superseded.

4.2.2 Personal Drives (P: drives)

- P: drives are a personal area for storing records relating to you in a work context e.g., timesheets; PDR documents. They can also be used to store very early drafts (when moved to a central area, drafts need to be deleted) or your own notes.
- They should **not** be used for corporate information, which must be stored on a shared drive or relevant system so that it is accessible to other team members.

- If you are a line manager, you may save information relating to staff or budget management on your P: drive.

4.2.3 Systems

- Where information needs to be uploaded to a relevant system (e.g., LiquidLogic, SAP), ensure that this is done as quickly as possible after being recorded or collected.
- Ensure appropriate access controls are set for personal and/or sensitive information so that only authorised individuals can view that information.

4.2.4 Laptops

- Only ever store information on a council owned encrypted laptop and only for short amounts of time.
- Limit the information stored on the laptop's desktop.
- Always adhere to the council's ICT Equipment Policy.

5.0 Disposing of Information

There are legislative or business requirements that govern the length of time some records must be kept. Always check the Corporate Retention Schedule before disposing of any records to determine whether a document needs to be retained.

PLEASE NOTE: In July 2015, the Chair of the Independent Inquiry into Child Sexual Abuse (IICSA) issued a moratorium on the destruction of files with content relating "directly or indirectly to the sexual abuse of children or to child protection and care." Knowingly destroying any such files could constitute a criminal offence under the Inquiries Act 2005. **Until further notice, teams must not destroy any records relating to children; services provided to children; and individuals who work(ed) with children**.

5.1 Paper

- **Never** dispose of documents containing personal or sensitive information in paper recycling bins.

- Dispose of personal or sensitive information securely using the confidential waste facilities, ensuring that these are shredded. Contact Custodians on 01452 42(5244) for confidential waste sacks or bins.
- When working at home personal or sensitive information can be shredded using a personal shredder; but the resulting shreds must then be disposed of using the council's confidential waste facilities.

5.2 Electronic

- Delete redundant, obsolete and trivial information (ROT) regularly.
- Information you have deleted from your desktop will be moved to the Recycle Bin. Ensure this information is permanently deleted by going into the Recycle Bin and clicking "Empty the Recycle Bin".

6.0 If you are moving to another role within the council, or are leaving GCC

- Before leaving your existing role, make arrangements to ensure that information remains available to those who need it. Ensure that business information you have access to is saved to a shared network, not kept in your P drive or emails. If you are a line manager who is changing roles/leaving, you will need to transfer information from your P: drive or emails to the individual taking over from you (or your line manager).
- If you are leaving the council:
    - Ensure that all GCC business information has been transferred from your P:drive and personal mailbox to an appropriate shared location, e.g. a network drive.
    - Delete any non-business information from your P: drive and all non-business emails from your mailbox.
    - Return all information and information assets (e.g., laptops, USB memory sticks).
    - If you are an Information Asset Owner or Manager, then inform Information Governance who will be replacing you in that role.
    - If you are the File Owner of records stored in the Records Centre, inform the Records Centre team who will be replacing you.

- If you are changing roles in GCC, your need for access to information and information systems is likely to change too. Line Managers **must** make arrangements to remove access rights from staff members who no longer need them. If you change roles and find that you still have access to information that you no longer have a need to access, you must flag this with your line manager and the ICT Service Desk.

7.0 Document Control

Owner:	Jenny Grodzicka, Head of Information Management
Authors:	Teresa Wilmshurst, IMS Team Manager (Records)
Create Date:	March 2019
Next review date:	November 2023
Version:	2.3

Version	Version date	Summary of Changes
2.3	October 2021	Format changes, updated out of date links