information management & security

Gloucestershire COUNTY COUNCIL

Clear Office Policy

1.0 Introduction

We all have an obligation to safeguard and maintain the confidentiality of the information that the council collects, holds, and manages. This policy outlines how having clear offices can support the security and confidentiality of information and describes the actions that all staff, including temporary staff and contractors, should take to achieve this.

The aim of this policy is to:

- Ensure that staff keep information secure, in line with our customers' expectations;
- Reduce the potential risk of information security breaches;
- Demonstrate that the council is taking corporate responsibility for the personal data in its care;
- Enable compliance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA);
- Help reduce the amount of paper storage required.

This policy also supports the following corporate policies:

- Information Security Policy
- Information and Records Management Policy
- Agile Working Principles

2.0 What is a "Clear Office"?

A "clear office" is more than just keeping your desk clear of unnecessary paperwork, although this is part of it. It means ensuring all areas, including kitchens and meeting rooms, are free from loose, unsecured paperwork, particularly when these areas are unattended. It also means ensuring that electronic information is not accessible to individuals within the office who are not authorised to view that information – this means having a "clear screen" when you are not working on ICT systems.

Material stored on your desk or in a cupboard is also a barrier to mobile working and makes it much harder for colleagues to find information in your absence. A properly structured filing system on SharePoint can be accessed in any GCC premises and by anyone with appropriate access rights.

A clear office also means keeping office spaces clean and hygienic. Avoid eating at your desk; instead, use the kitchen areas and cafés to have breakfast, lunch, and snacks. If you feel you haven't got a place to eat, please discuss your options with your manager.

3.0 The Policy in Operation

Maintaining a clear office requires all staff to follow some fairly straightforward steps:

3.1 Check and Clear

Paper

- ✓ All paperwork should be tidied away when not in use, with confidential or sensitive information, personal and special category data locked away securely;
- ✓ Ensure the desk you have been working on is clear of all paperwork when you leave it – this includes desks in hot-desking areas. If you are going to be away from your desk for more than half of your working day, clear the desk so that it can be used by colleagues;
- ✓ Always clear your desk before you go home. This includes tidying away personal items;
- ✓ Regularly check the storage units in your office for paperwork that may have become "lost" or "forgotten", especially if there are cupboards, pedestals and tambours that aren't used to store current records. Remember to pull drawers out to check that nothing has fallen behind or underneath them;
- ✓ Remember to check any "unseen" and/or "quirky" spaces within your office area and building – there may be attics; basements; roof voids where paperwork might have been left;
- ✓ Spaces such as windowsills; mantelpieces; meeting rooms; kitchens; floors under desks, and toilets must be kept free of any paperwork;
- ✓ Put a date and time in your diary to regularly sort out your paperwork to make sure you still need it;
- ✓ Always collect anything that you do have to print from MFD printers and scanners and other devices immediately. Never leave printouts on or by the machine;

- ✘ Don't leave boxes of files or loose paperwork unmanaged across your office space; these can end up becoming damaged or lost;
- ✘ Don't print off emails or other documents just to read them. This just generates increased amounts of clutter, increases the risks to information being lost or mishandled and increases your CO2 footprint!
- ✘ Don't leave any records you are using out of the office unattended. Ensure you follow the guidance for remote working with physical records.

Electronic Information

- ✓ Be aware of who can see the information on your screen as you work on it and where possible, move to a more private space when working on very sensitive information;
- ✓ Computers; laptops; tablets; and phones should be locked (press Ctrl+Alt+Del or Windows Key + L) when you are away from your workstation, or they are not in use.

- ✘ Don't leave mobile storage devices, such as DVDs and USB drives, out on desks. Instead, store them securely.

Store

- ✓ Take a digital first approach such as using business systems or SharePoint to store information appropriately for agile working;
- ✓ Think about who would need access to information if you were off sick and how they would be able to get access, e.g.:
  - ✓ Don't store working project papers, used by several colleagues, in your individual locker. Your colleagues won't be able to get hold of the information they need. Instead, store the documents in a filing cabinet that the appropriate people have access to;
  - ✓ Don't save electronic team documents on your OneDrive. In the event that you are absent, no one will be able to access them. See the M365 Acceptable Use Policy for more information on what should be stored on your OneDrive;
  - ✓ Scan and upload documents to systems and dispose of the original paper records once you've checked the quality, readability and usability of the electronic scanned document in accordance with GCC's Scanning Policy;
- ✓ Paper records that your team no longer need on a day-to-day basis but still need to be retained could be transferred to storage in the corporate Records Centre. All records with long term or historical value should be transferred to Gloucestershire Archives for permanent preservation;
- ✓ If you have to keep paper records locally store in an appropriate place, so that only the people who need access to the records have it. This means storing sensitive and confidential files in lockable storage units.

For more guidance, see the Information Protection and Handling Standards.

Dispose

- ✓ Consult the corporate Records Retention and Disposal Schedule to make sure you know what needs to be kept and for how long. Records for permanent preservation can be transferred directly to Gloucestershire Archives;

- ✓ All ROT* (redundant, obsolete and trivial) information should be disposed of as soon as possible;
- ✓ Always use the correct method to destroy paperwork. Never destroy paperwork through non-council waste facilities:
- ✓ All personal and/or sensitive information must be destroyed using the confidential waste facilities provided across the organisation, to ensure that this information is shredded;
- ✓ Paperwork that does not form a record of business activity and does not contain personal and/or sensitive information should be placed in recycling bins. This would include magazines, published material, and blank forms.

4.0 Security breaches

Leaving personal and/or sensitive information unattended, out for view, or lost and hidden may comprise **an information security breach** as it may breach the requirements set by the Data Protection Act 2018. If you become aware of a potential breach, report it immediately to the Information Security team.

5.0 Who can provide support with implementing this policy?

If you need help with implementing this policy, please see the contacts below for support:

- Should you identify a need for additional storage within your office area for paperwork you require access to on a day-to-day basis, this can be considered by emailing our Facilities Management (FM) Team: fm@gloucestershire.gov.uk.
- The Records Centre team can provide guidance and support with identifying and storing paper records that don't need to be retained in your offices: email recordscentre@gloucestershire.gov.uk or telephone ext. 4269.
- Gloucestershire Archives can help you with transferring records with long term or historical value to them: archives@gloucestershire.gov.uk.

* ROT is any information that you don’t need to keep. Examples of this include:

- Duplicates of information held elsewhere on the network drives or in another system;
- Information available elsewhere – such as publications from other organisations;
- File notes and initial drafts that have been superseded;
- Internal circulars and general information such as Talksmart emails.

6.0 Document Control

6.1 Document information

Owner:	Jenny Grodzicka, Head of Information Management Service (DPO)
Authors:	Teresa Wilmshurst, IMS Team Manager (Records) Kathryn Rhodes, Business Development and Performance Manager
Reviewer:	Teresa Wilmshurst, IMS Team Manager (Records)
Board(s) consulted:	Information Board
Date created:	December 2019
Next review date:	June 2027
Approval:	Rob Ayliffe, Director – Policy, Performance & Governance
Date of approval:	23 July 2024
Scheme of Delegation ref:	DPPG1
Version:	1.5
Classification:	UNCLASSIFIED

6.2 Version History

Version	Version date	Summary of Changes
1.0	December 2019	First version. Approved by Information Board, 11 December 2019.
1.1	October 2021	Updated out of date links
1.2	November 2022	Accessibility review and updates to formatting.
1.3	January 2024	Removed references to P: and S: drives and replaced with M365 equivalent
1.4	May 2024	Updated out of date links and contact details
1.5	June 2024	Broken links fixed following migration of Staffnet to SharePoint; updates to portable devices added; ROT information added as a footnote; amendments made to the wording of the storage section to emphasise electronic storage of information and new document information added.

6.3 Review

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

6.4 Contact Us

Post: The Information Management Service
Gloucestershire County Council
Shire Hall
Westgate Street
Gloucester
GL1 2TG

Email: dpo@gloucestershire.gov.uk

Phone: 01452 324000