Information Security Policy

This policy outlines the key principles to ensure that our information is kept securely, including office security; handling, transferring, and sharing information; and how to report suspected or actual data breaches.

Status of document: Approved
Version: 4
Date of approval: 30 January 2024
Effective from: February 2024
Owner: Senior Information Risk Owner
Author: Information Governance Officer
Planned next review date: February 2027

Contents

1. Office security – Office access keys

1.1 All employees, members, workers, contractors, and those working on our behalf are responsible for ensuring that our premises are left secure and there is no unauthorised access. This includes ensuring that doors are closed, that unknown individuals are challenged, and that visitors are accompanied.

1.2 The Facilities department is responsible for ensuring that all access keys are logged when issued to employees and/or members and that they are configured for each person, based on their access requirements.

1.3 Neither employees, members, contractors, nor workers should automatically be given full access to the office, especially to sensitive areas such as the server room.

2. Office security - Identification (ID) badges

2.1 Employees, members, workers, contractors, and visitors are required to always wear an identification badge and lanyard visibly, whilst on our premises.

2.2 All employees, members, workers, contractors, and visitors must be made aware of the requirement to always display their badge by Facilities and HR.

2.3 Employees, members, workers, contractors, and visitors will be provided with lanyards:

- Blue lanyards for employees,
- green lanyards for members, and
- red lanyards for visitors.

Only lanyards that are issued by us must be used.

2.4 Employees and members should challenge individuals without visible ID badges. All employees are encouraged to follow this good practice or, at a minimum, report those without ID badges to the Facilities manager or the Governance team.

2.5 Members are expected to wear their ID badges when conducting their GOC role at external venues and the GOC offices, for example, when visiting educational providers and within hearings.

2.6 Facilities maintain a register of ID badges detailing the date of issue, losses, and destruction for all employees and members, respectively. Facilities must arrange ID badges in advance of new starters joining the GOC, which are issued as part of the induction process within the first five days of joining.

2.7 New starters working in the office must be issued with a visitor pass daily by Facilities until their ID badge is issued.

2.8 If an employee, member, worker or contractor changes their job role, Facilities/Governance must ensure that a new ID badge is issued on the first day of the new role and that the old one is returned, logged, and disposed of securely.

2.9 Employees must return their ID badge to HR on their last day of service. Members, workers, and contractors must return their ID badges within their last week. Facilities will securely dispose of the ID badge and record its disposal.

3. Reporting loss or theft of ID badge or access key

3.1 Employees, members, workers, or contractors must immediately inform Facilities and the Information Governance Officer if their ID badge or Access Key is lost or stolen.

3.2 Facilities will immediately disable an individual's access key. The GOC reserves the right to charge individuals £20 for lost access keys.

3.3 Facilities will record the loss of the ID badge and issue another badge.

3.4 As the individual will need to report the loss in order to get a new badge/key, a security incident reporting form only needs to be completed if an actual data breach has occurred (e.g., unauthorised entry to the property) or if the individual has failed to report their badge/key was missing.

4. Visitors

4.1 Reception should be notified by email of visitors at least 24 hours in advance.

4.2 Visitors must report to reception on arrival and complete an entry in the visitor book, which will be stored out of sight.

4.3 Visitors will be provided with a visitor badge and a red lanyard, which they are required to wear in a visible position at all times whilst on GOC premises.

4.4 Visitors who are not working on behalf of the GOC (who have not signed a non-disclosure or a confidentiality agreement) must be collected from reception by the receiving employee and accompanied at all times when they are in our offices. They must never be left unsupervised, except for the reception area and public access areas.

4.5 Where it is impossible to accompany visitors at all times, all employees must be made aware of where they are working and the purpose of their visit.

4.6 Visitors must return their visitor badge and lanyard, and complete exit details in the visitor book upon leaving our premises.

5. Handling information

5.1 This section explains our approach to handling information safely. It includes our approach to:

- Information Storage (including Clear Desk and Clear Screen);
- Printing;
- Disposal; and
- Templates.

5.2 For further detail regarding these processes please consult the operational guidance, local instructions, or linked policies.

5.3 Information should be treated by all employees, members, workers, contractors, and those working on our behalf as they would wish their information to be treated.

5.4 Personal information (including business sensitive information) should not be shared or disclosed by employees and those working on our behalf in an unauthorised manner in any format.

5.4 All confidential, personal, or special category information in hardcopy or electronic form must be handled securely to mitigate the risk of unauthorised access.

Information Storage – Clear desk, clear screen, locked workstation

5.5 During the day, if a desk is not attended to, documents containing confidential, personal, or special category information must be put away in cupboards or pedestals.

5.6 Cupboards or pedestals containing confidential, personal, or special category information must be closed and locked when not in use or attended. Keys used to access secure cupboards must be returned to key storage and not left unattended.

5.7 Any removable media (e.g. USB sticks, DVDs) and documents containing confidential, personal, or special category information must be removed from desks at the end of each working day and kept securely.

5.8 Computers must be 'locked' when the desk is unoccupied and shut down at the end of the working day.

5.9 Care must be taken that the information displayed on all electronic devices is kept confidential, especially in public areas or public transport.

Printing

5.10 When printing confidential, personal, or special category information the 'locked' printing option must be used, and the individual printing must be in attendance.

5.11 Printers must be cleared of papers as soon as they are printed to make certain that confidential, personal, or special category documents are not left in printer trays.

Disposal

5.12 Confidential, personal, or special category documents, when no longer required, must be safely disposed of in confidential waste bins and care taken to ensure that the documents are fully inserted and not retrievable from the bins.

5.13 Meeting rooms must be immediately cleared of any documents containing confidential, personal, or special category data at the end of each meeting, this includes wiping down whiteboards and disposing of flip charts.

5.14 For more information about the disposal of archived information, please consult our Data Protection Policy.

Templates

5.15 Any templates used must be blank. Previously amended versions of templates must not be used as the base template, due to the risk of personal information being incorrectly included in the next use.

6. Transferring and sharing information safely

6.1 This section is about how to transfer data securely. For further information about when to share and when not to share information please refer to our Data Protection Policy and Disclosure Policy.

6.2 Always ensure the level of security is appropriate to the nature of the data being transmitted.

Transporting / on the move

6.3 Care must be taken at all times to ensure that all electronic and physical information is transported securely. This includes transporting laptops which are shut down so that the encryption code is still required and taking the appropriate measures such as putting sensitive documents in a lockable file for transport.

Posting

6.4 All post must be checked by the sender, before sending. The check must include:

- verification of the address on the envelope, letter, and the address held on file;

- verification that the information included is the correct information for the addressee;
- that any redaction has been fully completed and verified by another person; and
- that no further information has been included, due, for example, by an error in printing, scanning, or template use.

6.5 The Facilities team has set up mailing spreadsheets to record incoming and outgoing mail. This must be completed whenever you send or receive any post.

6.6 When posting confidential, personal, or special category information, use non- rip envelopes or double envelopes (ensuring name and address is on both envelopes), mark 'private and confidential or 'for the addressee only', and send via recorded delivery or courier.

6.7 To facilitate the appropriate management of the business, in general, Facilities may open any post that we receive at the GOC in order to establish the intended and appropriate receiver as long as it is reasonably addressed to the GOC.

6.8 For post that is marked 'private and confidential or 'for recipient only', which is addressed to the GOC, it would be handed to the Facilities Manager to open, sign, and record a reference. In their absence, our Facilities team would seek authorisation from the Head of Finance or Head of Governance.

Emails

6.9 All emails must be checked by the sender, before sending. The check must include:

- verification of the email address (sending a test email first if necessary);
- verification that the information included is the correct information for the addressee;
- that any redaction has been fully completed and verified by another person; and
- that no further information has been included, due, for example, by an error in the printing, template use, or previous email chain.

6.10 When sending emails, it is important to consider:

- who are the recipient(s), are they internal/external;
- might the message be intercepted if external;
- are previous emails included in the correspondence still relevant;
- do attachments require password protection or encryption;

and/or;

- the security marking of the email.
- where there are multiple recipients, use the "bcc" field to hide email addresses.

6.11 For additional security, senders should consider switching off their autofill on email addresses in outlook. This can be made mandatory by Information Asset Owners.

6.12 Senders should also consider including protective markings in the subject and body of the email and as the email setting, as appropriate.

6.13 For further information on electronic security measures, please refer to the IT Policy.

Verbal/over the phone

6.14 Users should ensure that they are not being overlooked or overheard if working on or discussing GOC business in public.

6.15 Telephone calls can often lead to unauthorised use or disclosure of personal data. It is mandatory to complete the following checks before releasing the data:

- Verifying the caller's identity – by asking questions only they would know, or by emailing or calling them back on the email/number we have on our IT system.
- If they are not the data subject and are requesting detail about someone else, you must not disclose information pertaining to the data subject, unless you have explicit consent from the data subject who will always have the right to withdraw their consent at any time in writing to the GOC. If in doubt, ask them to put their request in writing, or take their name and number and seek further advice from the Information Governance Officer or your line manager.

7. Removable media

7.1 We recognise that there are a number of risks associated with handling information, in particular those associated with the use of removable media, in order to conduct our functions. For this reason, removable media devices are prohibited unless there is a valid request that demonstrates a valid business use, which outweighs the associated risks and vulnerabilities, and the request has been approved in line with the IT Policy and process.

7.2 Removable media includes but is not limited to: media Cards; CDs; DVDs; external hard drives; USB memory sticks (also known as pen or flash drives); any other electronic storage devices.

7.3 Removable media must be treated like it is confidential, personal, or special category information and in line with the Data Protection Policy.

7.4 The process for obtaining and using removable media is managed by our IT department. Individuals must consider alternative, more secure arrangements, prior to requesting to use removable media.

7.5 Anyone using removable media devices to transfer data must consider the most appropriate way to transport the device and be able to demonstrate that they took reasonable care to avoid damage or loss, including encryption.

7.6 Only removable media devices supplied by our IT team may be used. Personal (non-GOC) removable media devices must not be used to store any GOC information and must not be used with any GOC-owned equipment.

7.7 Removable media provided by the GOC must not be used for anything other than the approved purpose. Only data that is authorised and necessary to be transferred should be saved on a removable media device.

7.8 Removable media devices must not be used for archiving or storing records as an alternative to the GOC network.

7.9 Removable media devices must be returned to the data subject once we no longer have a business need to retain it. If the data subject does not communicate that they want the device back, it will be destructed in line with our Data Retention Schedule policy.

Encryption

7.9 All data stored on removable media must be encrypted according to the GOC encryption standards, as provided by IT.

7.10 All data that is transferred to a third party via removable media must be on a GOC- supplied encrypted device.

7.11 Virus and malware checking software approved by IT must be operational on both the machine from which the data is taken and the device onto which the data is to be loaded.

8. Reporting an information security incident or near-miss

8.1 All employees, members, workers, contractors and those working on our behalf are expected to immediately report actual, suspected or potential breaches of information security. On discovery of the incident to the person who has discovered the incident must report it to their line manager (or their respective line managers if they are not available), the Information Governance Officer and their director immediately and via IG@optical.org.

8.2 Depending on the nature of the incident, the reporter may also need to inform the following person or people so that the matter can be most swiftly and appropriately managed:

Type of incident	Report to	Examples
IT / Cyber	Director of Corporate Services and IT	Virus, phishing attempts, lost laptops, iPads, or mobile phones, compromised passwords.
Physical security	Facilities Manager	Breaches of physical security – unauthorised entry on-site, lost access key.

8.3 This may include invoking the Business Continuity Plan or other policies.

8.4 Within 24 hours of becoming aware of the incident, the reporter must submit a security incident report form. This must then be sent to the Information Governance Officer. Failure to report within this timescale may be considered a disciplinary offence.

8.5 This is important because if the incident is a high risk, it may need to be reported to the ICO within 72 hours of the moment when someone first becomes aware (this can be the reporter, third party, etc.) of the breach.

8.6 The Information Governance Officer or the department manager will complete an investigation into the incident. If the incident is serious, conducting a full investigation in accordance with our internal Investigation Policy may be considered.

8.7 Any manager who is made aware of the breach as per this policy is expected to make all attempts to minimise the impact, in collaboration with the Information Governance Officer.

8.8 The Information Governance Officer will ensure that the following stages of breach management are completed in a timely manner, considering the ICO guidance on breach management:

- containment and recovery;
- assessment of ongoing risk;
- notification of breach;
  and;
- evaluation and response.

8.9 All Security Incident Reports will be signed off by the Data Protection Officer or deputy once an investigation has been completed.

8.10 The Data Protection Officer will decide whether any breach needs to be reported to the ICO, considering the ICO's guidance and will oversee its reporting, where required. Any ICO-reportable breaches need to be reported to the ICO within 72 hours of us becoming aware. Failure to do so can result in an automatic fine from the ICO.

8.11 Remedial and permanent measures to mitigate the risk of reoccurrence will be implemented by the appropriate department(s) who will be supported by the Information Governance Officer.

8.12 The Information Governance Officer will record all actions taken and lessons learned from the incident or near miss and will ensure these are periodically distributed within the organisation for continued learning and awareness.