

Information governance employee code of conduct and declaration

DOCUMENT CONTROL:

- **Version:** 1
- **Unique Reference number:** 1119
- **Approved by:** chief executive, director of corporate assurance
- **Date approved:** 1 October 2026
- **Document Author:** data protection officer and head of information governance
- **Title of Accountable Director:** director of corporate assurance
- **Date issued:** 1 October 2026
- **Review by date:** 30 September 2027

Contents

1. Document summary	3
2. Introduction and aim	4
3. Standards of conduct.....	4
3.1 Access information only for an authorised purpose.....	4
3.2 Protect confidentiality	5
3.3 Create and maintain accurate records	5
3.4 Share information appropriately	5
3.5 Use systems, devices and authentication securely	5
3.6 Email, messaging and correspondence	6
3.7 Remote, mobile and home working	6
3.8 Photographs, video and audio.....	6
3.9 Social media and public communications.....	6
3.10 New systems, applications, AI and local workarounds	7
3.11 Requests for information and individual rights.....	7
3.12 Report incidents and concerns immediately	7
3.13 Ask when unsure.....	7
4. Responsibilities	8
5. Training	8
6. Monitoring arrangements.....	9
7. Related documents and references.....	9
8. Appendices.....	9
8.1 Appendix 1: employee declaration	10
Declaration	10

1. Document summary

1.1 Why this Code is important

- The Trust uses information to give safe care and run its services.
- Information may be about patients, staff or the Trust.
- We must keep this information safe and private.
- These rules apply wherever you work. This includes working at home or travelling.

1.2 Only look at information you need

- Only look at information when you need it for your job.
- Do not look at records because you are curious.
- Do not look at your own record or the record of someone you know unless this is an approved part of your job.
- The Trust records and checks how systems are used.

1.3 Keep information safe

- Keep conversations private.
- Make sure other people cannot see your screen or papers.
- Check who a person is before you give them information.
- Share only the information they need.

1.4 Use Trust-approved email, systems, devices and storage

- Never share your password, passcode or smartcard.
- Lock your device when you leave it.
- Check the name, address and attachments before you send anything.
- Protect information when you work away from Trust buildings.
- Only use photos, video or sound recordings for an approved reason.
- Do not put confidential information on social media or personal accounts.
- Only use approved software and artificial intelligence tools.
- Check any work made with artificial intelligence. You are still responsible for the final work.

1.5 Ask for help and report concerns

- Send requests for personal or Trust information to the Information Governance team straight away.
- Report lost information, wrong access, cyber problems or other information incidents straight away.
- Do not hide or change evidence.
- If you are not sure what to do, stop and ask your manager or the Information Governance team.

Key message: Only access information needed for your work. Keep it confidential, accurate and secure. Use approved systems and processes. Share only when

appropriate and necessary. Report incidents and information requests promptly. Ask for advice when unsure.

2. Introduction and aim

This is a code of conduct and personal declaration. It sets out the information governance behaviours required of everyone working for or on behalf of the Trust. It is not a detailed policy or a substitute for role-specific procedures and training.

This Code sets the minimum standards for handling patient, service user, colleague, corporate and commercially sensitive information. Everyone within scope must read the Code, complete the declaration and follow the requirements throughout their work for the Trust.

The Trust relies on information to provide safe care, employ colleagues, manage services and meet its legal duties. People must be able to trust that their information will be used properly and protected from inappropriate access, use, alteration, loss or disclosure.

This Code applies whenever Trust information is handled, including when working on Trust premises, remotely, at home, while travelling, through email or messaging, and when using paper records, digital systems, photographs, video, audio, artificial intelligence or other technology.

The Code supports the seven UK GDPR principles: lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality; and accountability. It also supports the eight Caldicott Principles for confidential health and care information.

Detailed legal, clinical and technical requirements are contained in the related Trust policies, procedures and guidance. If this Code conflicts with an approved policy or specific professional requirement, seek advice from the Information Governance team before acting.

3. Standards of conduct

By signing the declaration, colleagues accept the following personal responsibilities.

3.1 Access information only for an authorised purpose

- I will access only the information needed to carry out my authorised duties and only for as long as the need exists.
- I will never search for, view or use records out of curiosity or personal interest.
- I will not access my own records, or records relating to relatives, friends, colleagues, acquaintances, public figures or other people known to me, unless formally authorised as part of my role and any conflict has been declared and managed.
- I will follow role-based access controls and immediately report access that appears excessive, incorrect or no longer required.

- I will understand that access to Trust systems is logged, monitored and may be investigated.

3.2 Protect confidentiality

- I will keep patient, service user, colleague, corporate and commercially sensitive information confidential during and after my work for the Trust.
- I will hold conversations where they cannot be overheard and position screens, papers and devices so information cannot be seen by unauthorised people.
- I will confirm identity and authority before discussing or disclosing information.
- I will use the minimum confidential information necessary for the purpose.
- I will not share confidential information through personal email, personal messaging accounts, unauthorised cloud storage or social media.

3.3 Create and maintain accurate records

- I will make records that are clear, relevant, factual, timely and attributable to me.
- I will distinguish fact, professional opinion and information reported by another person.
- I will correct errors through the approved process without concealing or improperly altering the original record.
- I will file information in the correct approved record or system and avoid duplicate or uncontrolled copies.
- I will follow the Trust retention schedule and never destroy, delete or retain information outside the approved arrangements.

3.4 Share information appropriately

- **I will** share information only where there is an appropriate care, operational, contractual or legal purpose and I am authorised to do so.
- **I will** apply the need-to-know and minimum-necessary principles and use an approved secure method.
- **I will** check recipients, addresses, attachments and sensitivity before sending information.
- **I will** record significant disclosure decisions where required, including the purpose, information shared, recipient and authority in accordance with Trust procedures.
- **I will** seek advice from my manager, Information Governance or the Caldicott Guardian where a disclosure is unusual, contested or difficult.

3.5 Use systems, devices and authentication securely

- I will use only my own account, smartcard, passcode, token or other authentication method and never share them or allow another person to use them.
- I will lock my device whenever it is unattended and keep Trust equipment physically secure.
- I will use only Trust-approved devices, software, applications, storage locations and communication channels.
- I will not install software, connect unapproved devices or bypass security controls.

- I will report lost devices, smartcards, credentials, suspicious messages, malware or unusual system behaviour immediately.

3.6 Email, messaging and correspondence

- I will use approved Trust communication systems for Trust business.
- I will check the intended recipient and use the minimum information necessary, particularly where names are similar or autofill is used.
- I will use secure transfer or encryption arrangements where required and obtain confirmation for urgent or sensitive information when appropriate.
- I will address paper correspondence clearly, package it securely and use the approved postal or courier method.
- I will not assume that sending information makes it received, read or acted upon.

3.7 Remote, mobile and home working

- I will work in a location that protects privacy and prevents unauthorised viewing, listening or access.
- I will use Trust-approved secure connectivity and follow current Digital and Information Security guidance.
- I will avoid printing or removing paper records unless authorised and necessary; where records are removed, track and transport them securely and return them promptly.
- I will not leave records or equipment visible or unattended in vehicles, public places or shared accommodation.
- I will protect confidential information from household members, visitors and other unauthorised people.

3.8 Photographs, video and audio

- I will only create, receive, view, store or share photographs, video or audio for an approved care or business purpose.
- I will use approved Trust equipment, systems and storage and follow any specific consent, confidentiality, safeguarding, clinical-record and retention requirements.
- I will ensure clinically relevant media is incorporated into, or appropriately referenced from, the official record and remove unnecessary duplicate copies from devices, inboxes or temporary storage.
- I will never post or disclose work-related media through personal accounts or social media.

3.9 Social media and public communications

- I will never identify a patient, service user or colleague, or disclose confidential Trust information, through social media, online forums or other public channels.
- I will follow professional-body requirements and the Trust social media and communications arrangements.
- I will understand that privacy settings do not make online content private and that reposting, screenshots and onward sharing may occur.

- I will not make discriminatory, defamatory, abusive or otherwise inappropriate statements connected with Trust work.

3.10 New systems, applications, AI and local workarounds

- I will not purchase, introduce, trial or use software, applications, cloud services, artificial intelligence tools, databases, spreadsheets or digital workarounds for Trust information outside the approved procurement and assurance process.
- I will ensure that the required information governance, data protection, cyber security, clinical safety, Digital Technology Assessment Criteria, procurement and contractual assurance processes are completed before processing starts.
- I will not enter patient, service user, colleague, confidential or commercially sensitive information into a tool unless that specific use has been approved.
- I will check AI-assisted content for accuracy, bias, confidentiality, completeness and appropriateness; remain responsible for the final work and decision.
- I will escalate proposed changes to the relevant manager and specialist teams early, before commitments are made or information is processed.

3.11 Requests for information and individual rights

- I will recognise that a request for personal information or exercise of an information right may be made verbally or in writing and does not need to mention legislation.
- I will forward subject access requests, rectification requests and other individual-rights requests to the Information Governance team immediately.
- I will forward Freedom of Information Act and Environmental Information Regulations requests for recorded corporate information immediately.
- I will not attempt to narrow, reject, disclose or otherwise determine a formal request unless authorised to do so.
- I will preserve relevant records when a request, complaint, investigation, claim or legal hold is known or anticipated.

3.12 Report incidents and concerns immediately

- I will report actual or suspected loss, inappropriate access, unauthorised disclosure, alteration, destruction, cyber incident or other information-security concern without delay through the approved incident route.
- I will act promptly to contain harm where safe and authorised, but not conceal, delete or alter evidence.
- I will co-operate openly with incident assessments and provide accurate information about what happened.
- I will report suspected deliberate misuse, unsafe practices or repeated non-compliance to my manager, Information Governance, Cyber Security or the Freedom to Speak Up route as appropriate.

3.13 Ask when unsure

Information governance decisions are often context specific. Colleagues must pause and seek advice where the purpose, authority, recipient, method, proportionality or security of

a proposed use or disclosure is unclear. A delay to obtain advice is preferable to an inappropriate use or disclosure of information.

4. Responsibilities

4.1 All colleagues

All colleagues must comply with this Code, complete required training and declarations, follow approved policies and local procedures, and raise concerns promptly.

4.2 Managers

Managers must make the Code available, ensure completion of training and declarations, provide appropriate supervision, maintain suitable access arrangements, act on concerns and seek specialist advice where required.

4.3 Information Asset Owners and system owners

Information Asset Owners and system owners must ensure access is authorised, proportionate, reviewed and removed when no longer required, and that information risks and controls are documented and monitored.

4.4 Specialist roles and teams

The Senior Information Risk Owner provides executive leadership for information risk. The Caldicott Guardian supports appropriate use and sharing of confidential health and care information. The Data Protection Officer advises on data protection compliance. Information Governance, Cyber Security, Digital, Clinical Safety, Procurement, Legal and other specialist functions provide assurance and advice within their remit.

5. Training

5.1 Data Security Awareness

- Audience: All colleagues
- Frequency: At induction and annually
- Delivery method: E-Learning via ESR

5.2 Role specific IG training

- Audience: Relevant roles
- Frequency: At induction and as required
- Delivery method: Briefing, workshop or approved learning with IG support

5.3 Code declaration

- Audience: All colleagues
- Frequency: At induction and materially revised
- Delivery method: Electronic or approved declaration

6. Monitoring arrangements

6.1 Training and declaration completion

- How: compliance reports reviewed by managers and responsible corporate function
- Report to: Relevant governance group and senior leaders
- Frequency: Quarterly

6.2 Information incidents and themes

- How: Incident data reviewed by Information Governance and Cyber Security
- Reported to: IG and Cyber governance arrangements
- Frequency: Regularly

6.3 Inappropriate access

- How: Risk-based and targeted audit by authorised system and assurance teams
- Reported to: Relevant manager, IAO, SIRO or governance route
- Frequency: Ongoing and as required

6.4 Rights requests performance

- How: Case monitoring by Information Governance
- Reported to: Relevant governance route
- Frequency: Regularly

6.5 Code effectiveness

- How: Feedback, audit findings, investigations and policy review led by Information Governance
- Reported to: Approving group
- Frequency: At review or sooner if required

7. Related documents and references

- Information Governance Policy and Management Framework
- Information Security Policy and related cyber security standards
- Records Management Policy and retention schedule
- Data Protection Impact Assessment Policy and guidance
- Information-sharing and disclosure guidance
- Incident reporting and management arrangements
- Acceptable use, remote working, email and social media policies
- Artificial intelligence governance, procurement and digital assurance arrangements
- Subject access, individual rights, Freedom of Information and Environmental Information Regulations procedures
- Professional codes of conduct and role-specific clinical or operational procedures

8. Appendices

8.1 Appendix 1: employee declaration

Important

This declaration confirms that the person signing has read and understood the Code and accepts the personal responsibilities it contains. It does not replace mandatory training, policies, professional standards or role-specific instructions.

Declaration

- I have read and understood the Information Governance Employee Code of Conduct and Declaration.
- I understand my personal responsibilities for protecting patient, service user, colleague, corporate and commercially sensitive information.
- I will only access, use and share information for an authorised purpose and in accordance with the need-to-know and minimum-necessary principles.
- I will use only approved systems, devices, applications, artificial intelligence tools and processes, and I will not introduce local workarounds outside the required assurance arrangements.
- I will keep information accurate, secure and in approved records and locations, and I will follow retention and disposal requirements.
- I will report actual or suspected incidents, inappropriate access, losses, information requests and other concerns promptly.
- I will complete mandatory and role-specific training, follow Trust policies and professional requirements, and seek advice whenever I am unsure.
- I understand that misuse of information, failure to protect confidentiality or failure to comply with this Code may result in restriction or removal of access, investigation, disciplinary action, referral to a professional body, legal action or criminal investigation, depending on the circumstances.
- I understand that these responsibilities continue after I leave the Trust.

Full name	
Job title	
Department or service	
Assignment or employee number	
Signature / electronic acknowledgment	
Date	