BANQUO
Part of Prospero Group

Confidentiality Policy

Date:	April 2025
Review date:	April 2026
Approved by:	Simon Buxton - Director

PROSPERO HEALTH & SOCIAL CARE
PROSPERO LEARNING
PROSPERO TEACHING

Contents

Confidentiality Policy

Policy Lead:	Simon Buxton - Director
Version No:	1.0
Date of issue:	April 2025
Date to be reviewed:	April 2026

Introduction

The purpose of this Confidentiality Policy is to set out the principles that must be observed by all who work within Banquo and have access to person-identifiable information or confidential information. All staff need to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in health and social care are bound by a legal duty of confidence to protect personal information they may come into contact with during the course of their work. This is not just a requirement of their contractual responsibilities but also a requirement within the common law duty of confidence and the Data Protection Act 2018.

It is important that Banquo protects and safeguards person-identifiable and confidential business information that it gathers, creates processes and discloses, in order to comply with the law, relevant mandatory requirements and to provide assurance to service users and the public.

This policy sets out the requirements placed on all staff when sharing information internally and externally (including NHS and Non-NHS Organisations).

Person-identifiable information is anything that contains the means to identify a person, e.g. name, address, postcode, date of birth, NHS number and must not be stored on removable media unless it is encrypted.

Confidential information within healthcare is commonly thought of as health information; however, it can also include information that is private and not public knowledge or information that an individual would not expect to be shared. It can take many forms including service user level health information, employee records, occupational health records, etc. It also includes our organisational confidential business information.

Information can relate to service users and staff (including temporary staff), however stored. Information may be held on paper, CD/DVD, USB sticks, computer file or printout, laptops, palmtops, mobile phones, digital cameras or even heard by word of mouth.

Scope

This policy applies to all Banquo staff and agents acting on behalf of the organisation.

Roles and responsibilities

Confidentiality is an obligation for all staff. There is a confidentiality clause in their contract and that they are expected to participate in induction, training and awareness-raising sessions carried out to inform and update staff on confidentiality issues.

Specific roles and responsibilities are outlined within the Information Governance Framework (see Information Governance and Record Keeping Policy).

Any breach of confidentiality, inappropriate use of health, staff records or business sensitive/confidential information, or abuse of computer systems is a disciplinary offence, which could result in dismissal or termination of employment contract and must be reported in line with Banquo's Information Governance and Record Keeping Policy.

Key principles

All staff must ensure that the following principles are adhered to;

- Person identifiable or confidential information must be effectively protected against improper disclosure when it is received, stored, transmitted or disposed of;
- Access to person-identifiable or confidential information must be on a need-to-know basis;
- Disclosure of person identifiable or confidential information must be limited to that purpose for which it is required;
- Recipients of disclosed information must respect that it is given to them in confidence;
- If the decision is taken to disclose information, that decision must be justified and documented;
- Any concerns about disclosure of information must be discussed with a member of the Senior Leadership Team

Banquo is responsible for protecting all the information it holds and must always be able to justify any decision to share information.

Person identifiable information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of the data.

Within Banquo's office space, access to where person identifiable or confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card.

Banquo has a clear desk policy, due to desk sharing, all staff should clear their desks at the end of each day. In particular staff must keep all records containing person-identifiable or confidential information in recognised filing and storage places that are locked.

Unwanted printouts containing person-identifiable or confidential information must be put into a confidential waste bin. Printouts, USB Sticks and other removable devices must not be left lying around but be filed and locked away when not in use.

Banquo's Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

Disclosing personal/confidential information

To ensure that information is only shared with the appropriate people in appropriate circumstances, care must be taken to check they have a legal basis for access to the information before releasing it.

It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

Information can be disclosed:

- When effectively anonymised in accordance with the Information Commissioners Officer Anonymisation Code of Practice;
- When the information is required by law or under a court order. In this situation staff must discuss with the Registered Manager or other staff with roles within Information Governance before disclosing, who will inform and obtain approval of the Caldicott Guardian;
- In Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with the Registered Manager or Information Governance staff before disclosing, who will inform and obtain the approval of the Caldicott Guardian;
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with the Registered Manager or Information Governance staff before disclosing, who will inform and obtain approval of the Caldicott Guardian.

If staff have any concerns about disclosing information, they must discuss this with the Registered Manager, or the Information Governance team.

Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing/Information Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer.

Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail.

Transferring service user information by email to anyone outside the organisation, may only be undertaken by using encryption or through an exchange within a secure system, since this ensures that mandatory government standards on encryption are met. Sending information via email to service users is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

Working away from the office environment

If staff are working away from the office environment and need to carry organisational information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents they also have a duty to manage data securely and maintain confidentiality.

Taking home paper documents that contain person-identifiable or confidential information is discouraged.

To ensure safety of confidential information, information must always be kept on their person whilst travelling and kept in a secure place if taken home or to another location. Confidential information must always be safeguarded and kept in lockable locations.

Staff must ensure that their working practice complies with organisational policies and procedures.

If staff do need to carry person-identifiable or confidential information they must ensure the following:

- Any personal information is in a sealed non-transparent container i.e. windowless envelope, suitable bag, etc. prior to being taken out of our buildings.
- Confidential information is kept out of sight whilst being transported.

If staff do need to take person-identifiable or confidential information home, they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

Staff must NOT forward any person-identifiable or confidential information via email to their home e-mail account.

Staff must not use or store person-identifiable or confidential information on a privately owned computer or device.

Carelessness

All staff have a legal duty of confidence to keep person-identifiable or confidential information private and not to divulge information accidentally.

Staff may be held personally liable for a breach of confidence and must not:

- Talk about person identifiable or confidential information in public places or where they can be overheard;
- Leave any person-identifiable or confidential information lying around unattended, this includes telephone messages, computer printouts, faxes and other documents;
- Leave a computer terminal logged on to a system where person-identifiable or confidential information can be accessed, unattended.

Steps must be taken to ensure physical safety and security of person identifiable or business confidential information held in paper format and on computers.

Passwords must be kept secure and must not be disclosed to unauthorised persons. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. If you allow another person to use your password to access the network, this constitutes a disciplinary offence and is gross misconduct which may result in your dismissal.

Abuse of privilege

It is strictly forbidden for employees to knowingly browse, search for or look at any personal or confidential information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act.

When dealing with person-identifiable or confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of the organisation.

If staff have concerns about this, they should discuss it with the Registered Manager.

Confidentiality audits

Good practice requires that all organisations that handle person-identifiable or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and procedures to evaluate the effectiveness of controls within these systems. This function will be co-ordinated by the Data Protection Officer through a programme of audits.

Distribution and implementation

This document will be made available to all Staff.

A global notice will be sent to all Staff notifying them of the release of this document.

Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the Data Protection Officer, together with independent reviews by both Internal and External Audit on a periodic basis.

The Data Protection Officer is responsible for the monitoring, revision and updating of this document on a yearly basis or sooner if the need arises.

Related Policies and Procedures

Information Governance and Record Keeping Policy and Procedures

Quality, Governance and Risk Policy and Procedures

Incident Management Policy

Legislation and Guidance

Data Protection Act 2018

Freedom of Information Act 2000

UK General Data Protection Regulation

Privacy and Electronic Communications (EC Directive) Regulations (PECR) 2003

Private and Voluntary Health Care (England) Regulations 2001

The Information Governance Review (publishing.service.gov.uk)

UK GDPR guidance and resources | ICO

information-security-policy-v4.0.pdf (england.nhs.uk)

The Private and Voluntary Health Care (England) Regulations 2001 (legislation.gov.uk)

Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk)

Appendix A: Confidentiality Dos and Don'ts

Do

- Do safeguard the confidentiality of all person-identifiable or confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of the organisation.
- Do clear your desk at the end of each day, keeping all portable records containing person-identifiable or confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.
- Do switch off computers with access to person-identifiable or business confidential information, or put them into a password-protected mode, if you leave your desk for any length of time.
- Do ensure that you cannot be overheard when discussing confidential matters.
- Do challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know.
- Do share only the minimum information necessary.
- Do transfer person-identifiable or confidential information securely when necessary i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.
- Do seek advice if you need to share service user/person-identifiable information without the consent of the service user/identifiable person's consent and record the decision and any action taken.
- Do report any actual or suspected breaches of confidentiality.
- Do participate in induction, training and awareness-raising sessions on confidentiality issues.

Don't

- Don't share passwords or leave them lying around for others to see.
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible.
- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

Appendix B: Summary of legal frameworks

The organisation is obliged to abide by all relevant UK legislation. The requirement to comply with this legislation shall be devolved to employees and agents of the organisation, who may be held personally accountable for any breaches of information security for which they may be held responsible.

Legislation and guidance

Data Protection Act 2018 regulates the use of "personal data" and sets out six principles to ensure that personal data is:

1. requirement that processing be lawful and fair;
2. requirement that purposes of processing be specified, explicit and legitimate;
3. requirement that personal data be adequate, relevant and not excessive;
4. requirement that personal data be accurate and kept up to date;
5. requirement that personal data be kept for no longer than is necessary;
6. requirement that personal data be processed in a secure manner.

The Caldicott Report (1997) and subsequent Caldicott or National Data Guardian reviews recommended that a series of principles be applied when considering whether confidential service user-identifiable information should be shared:

- Justify the purpose for using service user-identifiable information.
- Don't use service user identifiable information unless it is absolutely necessary.
- Use the minimum necessary service user-identifiable information.
- Access to service user-identifiable information should be on a strict need to know basis
- Everyone should be aware of their responsibilities
- Understand and comply with the law.
- The duty to share information can be as important as the duty to protect service user confidentiality.

Article 8 of the Human Rights Act (1998) refers to an individual's "right to respect for their private and family life, for their home and for their correspondence". This means that public authorities should take care that their actions do not interfere with these aspects of an individual's life.

The Computer Misuse Act (1990) makes it illegal to access data or computer programs without authorisation and establishes three offences:

1. Unauthorised access data or programs held on computer e.g. to view test results on a service user whose care you are not directly involved in or to obtain or view information about friends and relatives.

2. Unauthorised access with the intent to commit or facilitate further offences e.g. to commit fraud or blackmail.

3. Unauthorised acts the intent to impair, or with recklessness so as to impair, the operation of a computer e.g. to modify data or programs held on computer without authorisation.

Common law duty of confidentiality

Information given in confidence must not be disclosed without consent unless there is a justifiable reason e.g. a requirement of law or there is an overriding public interest to do so.

Administrative law

Administrative law governs the actions of public authorities. According to well established rules a public authority must possess the power to carry out what it intends to do. If not, its action is “ultra vires”, i.e. beyond its lawful powers.