BrisDoc Patient care by people who care

NHS

Information Governance Staff Handbook

Version:	**Owner:**	**Created:**
1.0	Deb Lowndes (Programme and Service Director.)	March 2021
Published:	**Approving Director:**	**Next Review**
23/06/2025	Rhys Hancock (Director of Nursing, AHPs and Governance.)	23/06/2026

Contents

Introduction

This handbook supports staff to understand and apply BrisDoc's approach to data protection, information governance (IG), and cyber security. It complements our Data Protection Policies (available on Radar) and outlines key responsibilities and best practices for all staff.

All staff have a responsibility to protect the confidentiality, integrity and availability of patient and organisational data. This guide aims to:

- Explain key legal duties and governance principles
- Provide practical tips to support your day-to-day work
- Reduce risk by improving awareness and promoting good habits

If in doubt, call it out. Raise concerns with your manager or via the Learning event portal.

Legal and Organisational Responsibilities

Legislation and Standards

Data protection legislation includes:

- Data Protection Act 2018
- UK GDPR
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- Health and Social Care Act 2012
- Records Management Code of Practice (2021)

BrisDoc is also expected to comply with:

- The NHS Data Security and Protection Toolkit (DSPT)
- Guidance from the Information Commissioner's Office (ICO)

Key Roles

- SIRO: Senior Information Risk Owner – overall accountability for information risk. This role is held by the Programme and Service Director.
- Caldicott Guardian: Responsible for protecting patient and staff confidentiality. This role is held by the Medical Director.
- Data Protection Officer: Provides independent advice and oversight. This role is outsourced by BrisDoc to Regulatory Solutions.
- Information Security Lead: Ensures cyber security standards are met. This role is held by the Programme and Service Director.

Support is provided by Heads of Service and Corporate Leads. These roles form the Information Governance Board.

Key Principles

BrisDoc staff must follow:

- Data Protection Principles (fairness, transparency, minimisation, security, etc.)
- Caldicott Principles (need-to-know, minimal use, audit access, etc.)

Staff must:

- Not discuss personal data in public areas
- Never access records without a legitimate purpose
- Report any breach or suspected incident immediately

Practical Guidance for Staff

Core Good Practice for All Staff

Passwords

- Use strong passwords (e.g. three random words)
- Do not share passwords or write them down

Smartcards

- Always keep your card and password safe.
- If you lose your card inform your line manager immediately.

Physical Security

- Keep desks tidy and paper-free
- Lock screens when away from your computer
- Challenge unaccompanied visitors

Digital Security

- Double-check email recipients
- Only send sensitive information to NHS.net or secure systems
- Never click suspicious links – delete and report phishing attempts

Think Before You Click – the most common way ransomware enters networks is through email.

To avoid this trap, please observe the following email best practices:

- Do not click on links or attachments from senders that you do not recognise
- Be especially wary of .zip or other compressed or executable file types
- Do not provide sensitive personal information (like usernames and passwords) over email
- Watch for email senders that use suspicious or misleading domain names
- If you cannot tell if an email is legitimate or not, please delete it and raise a digital support ticket

If something seems wrong, DELETE IT. If it is legitimate, they will email again.

Telephone Security

- Confirm the identity of the caller and justify the need to disclose confidential information to them before doing so. If in doubt, ask for something in writing or that you will call them back.

Devices

- Keep Laptops secure and in your possession

Public WiFi

- Avoid using public WiFi for work
- Use a mobile hotspot or VPN if remote access is essential

Reporting

- Report all incidents or near-misses via Learning event portal.
- Contact your manager or the Digital Team

Supporting a Safe Culture

Training and Awareness

- Annual IG training is mandatory for all staff
- Keep updated with changes to policies and SOPs

Incident Types to Report

- Lost or stolen devices
- Misdirected emails or letters
- Unauthorised access to records
- Malware or phishing attempts

Cyber Hygiene Tips

- Don’t use personal devices for work unless authorised
- Avoid using work devices for personal browsing
- Be alert to unusual system behaviour

Summary

- Information Governance is everyone’s responsibility
- Ask if unsure. Report concerns quickly
- Follow the principles and good practice outlined here

Version Control

Date	Version	Author	Change Details
March 2021	1.0	DL	First draft
May 2021	1.1	DL	Comments from NC and SP
July 2021	1.2	DL	Final version for issue
August 2021	1.3	DL	KR Review
March 2022`	1.4	DL	Addition of info re public wifi use
23/06/25	1.0	DL	Published as V1.