BrisDoc Patient care by people who care

NHS

BrisDoc Digital Acceptable Use Policy

Version:	Owner:	Created:
1.0	Nero Namdhari	28/11/2025
Published:	**Approving Director:**	**Next Review**
08/12/2025	Deb Lowndes (Programme and Service Director.)	08/12/2026

Contents

Introduction

This policy sets out the acceptable and unacceptable uses of BrisDoc's Information Communication Technology (ICT) resources.

It forms part of our Information Governance Management System (IGMS) and aligns with the wider information governance framework, including the Data Security and Protection Toolkit. Compliance with the Toolkit is essential for the organisation to gain and maintain access to NHS systems such as the Health and Social Care Network (HSCN), NHS Mail, MS Teams, limited N365 applications, Spine, and clinical applications.

BrisDoc operates a Zero Trust security model. This means no user, device, or system is trusted by default, whether it is inside or outside our network. Each request for access is verified and granted only with the minimum permissions required, supported by appropriate conditional access controls.

We apply continuous authentication and consistent security checks to safeguard patient data, business information, and NHS systems. While this approach can feel more stringent than traditional IT security, it significantly reduces cyber risk and supports our compliance with NHS and legal requirements.

Scope

This policy covers the following areas of ICT use:

- Responsibilities and use of Information Technology (IT) assets
- Use of email and internet
- Use of mobile devices, removable media, and remote access
- VOIP telephony
- Network usage (including passwords and user access control)
- Use of patient information
- Use of AI systems

This version supersedes all previous versions of this document.

This policy specifically applies to all SevernSide and Corporate BrisDoc HealthCare Services staff, across all its operating locations (namely remote working staff both Nationally and Internationally (SevernSide Clinicians only via our approved governance approach) Out Of Hours Urgent Treatment Centres, Staff from Trusted Partner Organisations, Contractors and Vendors associated with the organisation) and any other authorised user of BrisDoc's Managed Network or devices.

The principles also apply to BrisDoc Practice Services staff, however there are local policy and procedures that are specific to Practices Services due to the nature of the Digital provision by NHS England. Staff should refer to their line manager for further information.

It describes the responsibilities and acceptable use of ICT and Information assets hosted or accessed by BrisDoc HealthCare Services.

A failure to follow the requirements of this policy may result in investigation and management action being taken as considered appropriate. This may include formal action in line with the organisation's disciplinary procedures for employees; and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment, or honorary agreement.

Non-compliance may also lead to civil or criminal action being taken.

Ownership and Responsibilities

Roles of Managers

Line Managers are responsible for:

- Identifying the systems and levels of access that their staff need to be able to undertake their duties and inform Digital so that access control is maintained.
- Annually reviewing your staff's systems access needs to ensure that it is still required, as part of the Information Assets and Data Flows review required for compliance to the Data Security and Protection Toolkit.
- Responsible for the information assets within their role and/or department and act as the data custodians/data stewards but are not Data Controllers. BrisDoc remains the Data Controller.
- Ensuring that department/service information is transferred from personal network folders (such as the H:/ drive) One Drive, Emails, and laptops to the appropriate shared folders when a member of staff leaves to ensure data protection and business resilience.
- Ensure any Business loan equipment e.g., Laptops, phones and ID badges are returned to the Digital Team.
- Notify the Digital Team when staff have gone on long term sick, leave, maternity or sabbatical. This is so that access to emails can either be disabled or transitioned to another member of staff to maintain business functions in line with BrisDoc policy.

Role of the Information Governance Board

The Information Governance Board are responsible for:

- Reviewing the Policy.
- Ratifying the Policy.
- Receiving reports highlighting risks and incidents relating to breaches of this policy.

Role of Digital Team

The Digital Team are responsible for:

- Maintaining the hardware and software components of the Digital and communications infrastructure.
- Implementing all necessary technical and physical security controls to protect Digital related Information Assets.
- Digital implements technical access control based on approval from the relevant Information Asset Owner.

- Ensuring sufficient systems and processes are in place to monitor ICT activity to ensure compliance with Digital policies, NHS standards, and UK Law.
- Ensuring all new user accounts are created and accounts for those staff who have left are closed off in a timely manner.
- Raising concerns/issues should adherence to this policy be breached.

Role of the Information Asset Owners

The appointed information Asset Owner (IAO) will be responsible for each logical or physical set of information assets relating to software or applications and those generated by business processing. IAO's are responsible for:

- Understanding what information is held and where it's located.
- Knowing what is added, moved or removed.
- Understanding how information is moved.
- Knowing who has access and why and what the access controls are and that they are applied appropriately.
- Determine and approve access requirements; Digital enforces these through technical controls.
- Knowing the retention schedule of the asset.
- Reporting all changes back to the SIRO via an updated Information Asset and Data Flows log.

Role of individual staff

Digital systems are a business tool that should be treated like any other tool in the workplace. Staff and contractors should be aware that their line manager and colleagues may need to gain access to an individual's Digital systems under certain circumstances (e.g. authorised need during absence). Staff and contractors are therefore advised to carefully consider the use of BrisDoc's provided Digital systems for personal use.

All Staff members are responsible for:

- Ensuring that they have read and understood this policy. Clarification as to what is Acceptable Use can be obtained from your Line Manager or Digital Team.
- Ensuring that any usage conforms to policy and legislation relating to Digital security, confidentiality, and data protection.
- Manage their NHS mailbox in accordance with NHSmail Acceptable Use Policy (AUP) and NHS Code of Practice.

Standards and practice

Acceptable Use – General

Access to Digital systems is primarily for business related purposes – to support (directly or indirectly) the provision of healthcare.

Personal access to Digital systems can be limited or denied by your manager. Staff and contractors must act in accordance with organisational Policies and their manager's locally imposed restrictions.

Never leave your computer logged in whilst unattended, always log out or lock the screen before leaving, even if it is only briefly.

Personal Corporate Devices - Identity, Passwords, Password Managers, Smart Cards, and BitLocker

Each user is assigned a unique login.

As an organisation BrisDoc uses a combination of the above listed types of authentications to secure its systems. All passwords should be unique and be made up on three random words and should aim to be at least twelve characters long. However other systems may require password lengths of 8 or 10 characters or longer.

Never give your password or PIN to anyone else. If you feel your password has been compromised, then change it immediately and contact the Digital Team.

Never repeat a password by adding incremental digits when requested to change.

Each user is responsible for maintaining the security of their individual login and password. Staff and contractors must not share their username or password with anyone. Misuse of a user's account will be investigated and may lead to disciplinary action. This includes staff and contractors that have remote access to the business systems. Never write passwords down, if you find it hard to remember your password, write a clue as an 'aide memoire' or use a password Manager.

MFA / 2FA – Where applicable please secure your password with either multifactor authentication or two factor authentication.

Password Managers – where possible please use a Password Manager. All business passwords are stored in Bitwarden, and access control is managed by the Digital Team.

Staff and contractors should log out when finished with Digital IT systems. If a computer is found to be still logged in when you try to use it, you should always log the computer out and then log in using your own account details.

Smart Cards – All users who are issued smart cards are responsible for complying with the National Smart Card terms and conditions.

Never loan your smart card to another person or disclose your PIN.

Always remove your smart card from the reader when not in use and keep it secure.

BitLocker – if you have been assigned a business laptop this will secured with a 6-digit PIN or a password of BrisDoc's choosing. Never give this PIN or password to another person and keep it secure.

Digital equipment

BrisDoc uses a mix of desktop computers, laptops, and mobile phones. All users of BrisDoc's Digital equipment must adhere to the following points.

- Users are responsible for safeguarding issued devices e.g., laptops and mobile phones.
- Users must comply with the guidance supplied for the management and maintenance of devices.
- Equipment must be locked when unattended.

- Data must be stored using authorised systems (e.g. shared network drives).
- Equipment must be returned upon departure from the organisation.
- All users must report any damage, alerts, or security notifications to the Digital Team.

Physical Security of Mobile Devices

- Devices must be physically secured when not in use, and screens must be locked.
- Equipment must not be left unattended in vehicles unless locked in the boot or stored in secure compartment.
- Devices should not be left in public view or unattended workspaces.
- For information see the Mobile Computing Policy.

Internet and Email

- Email and internet access are provided primarily for BrisDoc business purposes, as well as professional development and training that align with the organisation's goals and objectives.
- Limited personal use is permitted, provided it does not interfere with your own duties or the responsibilities of other BrisDoc HealthCare Services staff. Such usage must never disrupt colleagues or impact operational performance.
- All staff should ensure these systems are used for legitimate BrisDoc business activities and always within the scope of their authority.

Use of AI

BrisDoc supports the use of AI to improve efficiency and care, but it must be safe, secure, and compliant with UK GDPR, the Data Protection Act 2018, the Common Law Duty of Confidentiality, the Caldicott Principles, NHS England's Data Security and Protection Toolkit, NHS England's guidance on AI assurance, UK DSHC's "Safe, Secure, Effective" framework, and relevant NHS clinical-safety standards (DCB0129 and DCB0160). These standards apply where AI forms part of a clinical system or influences clinical decision-making.

- Approved Tools Only: Use AI systems authorised by BrisDoc's Digital Team.

- Protect Data: Do not upload patient or confidential information to public or unapproved AI platforms.

- Support, Not Replace: AI should assist decision-making, not replace professional judgement.

- Security: Ensure AI tools do not introduce risks such as malware or data leaks.

- Monitoring: AI use may be reviewed for compliance.

- Follow Guidance: Always follow BrisDoc's AI Guidance Policy.

Remote and Home Working

- All remote working requests must be made through your line Manager for corporate employees and for SevernSide through Service Delivery Teams process.

- BrisDoc supports the use of personal devices by SevernSide remote clinicians exclusively for remote working. Support is limited to the secure connection method approved and configured by BrisDoc. Device owners are responsible for ensuring their devices comply with BrisDoc requirements, including up-to-date operating systems, security patches, antivirus protection, and reliable connectivity. BrisDoc may remove access if a personal device is found to be non-compliant with these requirements.
- Corporate supplied devices are subject to a device management approach shared and agreed by the user at the time of issuing the device.
- Only approved remote working solutions are permitted, and this is managed by the Digital Team.
- All devices either personal or company must be secured against unauthorised access. Staff with personal devices must not store business data on their personal devices. If found this will be classed as a breach of business data.
- Public computers, hotspots etc must not be used to access corporate systems.
- Where required, approved encryption must be used for sensitive data.

Permitted and Prohibited Uses

- You must not use the internet for any gambling or illegal activity, including for personal business.
- BrisDoc may use automated content filtering software to restrict the access to categories that are deemed to be inappropriate e.g., violence, criminal, adult/sexual etc content. These are subjected to ongoing review. However, BrisDoc does recognise that we cannot block everything. Access to a website does not imply that its use is permitted.
- Downloading of Non – Business approved applications – All applications must be in line with BrisDoc's software onboarding and approval process and must align with the Privacy by Design Policy.
- It is an offence under the Computer Misuse Act 1990 – to knowingly introduce malware, virus, botnets, worms etc to disrupt business.
- All users of BrisDoc systems are advised to not store personal or confidential information/data in unauthorised locations.

Social media, Blogging, Tweeting etc

- Protect Reputation: Do not post content that could harm BrisDoc's reputation or misrepresent its views.
- Confidentiality: Never share patient information, internal business details, or sensitive data on social platforms.
- Personal vs Business Use: Personal accounts must not be used for official BrisDoc communications. Business-related posts should only be made through authorised channels.
- Professional Conduct: avoid expressing personal opinions on professional matters in a way that could be interpreted as BrisDoc's position.

- Refer to BrisDoc's social media Policy for further detail.

Data protection and Confidentiality

- All users of BrisDoc's systems are responsible for handling data in line with business practices and legislation i.e. GDPR and Data Protection Act 2018
- Avoid displaying confidential information in public spaces.
- When authorised remote support is being provided, please close or minimise any windows containing sensitive information.
- Where possible, all users should refrain from sending confidential, sensitive information i.e., PID in email. However, in certain cases we recognise that this is unavoidable. In such cases information should be sent via NHS Secure email option.
- If you work with BrisDoc Tenant i.e. if your email address uses the @brisdoc.org domain, please speak to Digital about secure sending of emails.
- Other recognised methods of secure data transfer are SFTP by authorisation of Digital Team only.
- For further information please see the organisation's Information Governance Procedures.

Security, Cyber Security & Monitoring

- All BrisDoc devices have security tools installed to protect them and the wider business.
- All data traffic passing through business networks systems such as Guest-wireless, corporate wireless and physical connected devices are subject to appropriate security controls, including firewall filtering.
- To further ensure compliance, data protection and detect misuse all BrisDoc systems may be monitored and recorded. Monitoring will be lawful, proportionate and only accessed by authorised personnel.

Training

All users must:

- Complete annual information governance training via the BrisDoc Development Hub.
- Confirm receipt of key policies during induction.
- Participate in any additional role-specific training required.

Incident Reporting

All staff must report any actual or suspected information security incident immediately. This includes, but is not limited to:

- Lost or stolen devices (e.g., laptops, mobile phones, smart cards)

- Suspected data breaches or unauthorised access
- Malware infections or suspicious system behaviour
- Accidental disclosure of confidential information
- Misuse of BrisDoc systems or credentials

Reporting Process:

1. Notify your Line Manager as soon as possible.
2. Contact the Digital Team immediately.
3. For serious incidents (e.g., involving patient data or significant system compromise), escalate to the Senior Information Risk Owner (SIRO) without delay.
4. Complete a Learning Event Form via the Learning Events Portal.
5. Do not attempt to fix or conceal the issue yourself—preserve evidence where possible.

Why Reporting Matters: Prompt reporting helps BrisDoc protect patient data, maintain compliance with NHS standards, and reduce organisational risk.

Compliance and Enforcement

Breaches may lead to:

- Disciplinary action
- Suspension of Digital access
- Legal proceedings in serious cases

Compliance will be monitored through incident reporting, audit, and training records.

Appendix A - Definitions / Glossary

- **2FA**: Two-Factor Authentication – a type of MFA using two verification steps.
- **Access Control**: Methods to restrict access to systems and data based on user roles and permissions.
- **AI**: Artificial Intelligence – technology that simulates human intelligence for tasks like analysis and automation.
- **AUP**: Acceptable Use Policy – rules for using BrisDoc's IT systems responsibly.
- **Applications/Software** – Computer programs designed to store and manipulate information to support or provide a service.
- **Archive/Archived (Cold Storage)** – Information that is no longer current which is retained to allow future access should the need arise. This may mean the information is moved to slower devices or compressed but will still be accessible.
- **Availability** – Ensuring that information is available at point of need for those authorised to access the information.
- **Business Continuity**: Plans and processes to keep services running during disruptions.
- **Backup** – A copy (or the activity to produce a copy) of data stored on a computer.
- **Batch Processing** – The manipulation/updating of information done after the event that initiated the change. Where changes cannot be implemented at the time that they happen, they are stored and collected to be updated at a later pre-determined time.
- **BitLocker** – Is an encryption mechanism used to secure computer hard drives and / or boot systems. This adds an added layer of defences and is used on all our laptops.
- **Blogging (or Tweeting)** – This is using a public website to write an on-line diary (known as a blog) or sharing thoughts and opinions on various subjects. Blogs and Tweets are usually maintained by an individual with regular entries of commentary, descriptions of events, and may include other material such as graphics or video Examples of blogging websites include X.com and Blogging.com.
- **Business Continuity** – The activity performed by an organisation to ensure that services are available to patients and staff.
- **Cloud / Cloud computing** – "Cloud" is another term to describe the Internet. Cloud computing refers to services that are available in the cloud or on desktop or mobile apps with connectivity to services in the cloud.
- **Confidentiality** – Ensuring that personal, sensitive and/or business critical information is appropriately protected from unauthorised access and is only accessed by those with an approved need to access that information.
- **Cyber** – Involving, using, or relating to computers, especially the internet.
- **Cyber Bullying** – Cyber harassment or online bullying. A form of bullying or harassment using electronic means. Cyberbullying is when someone bullies or harasses others on the Internet, particularly on social media sites.
- **Cyber Security** – Is a term to cover defence against attacks primarily from the internet. These attacks can take many forms from direct hacking attempts, emails containing malware or links to infected websites, etc.

- **Critical Communications (Comms) Room** – Network communication room (or cabinet) that is relied upon to provide access and availability to BrisDoc's critical clinical and business systems.
- **Data Protection**: Safeguarding personal and sensitive data from misuse or unauthorised access.
- **Disaster Recovery**: Steps to restore systems after a major failure or incident.
- **DSP**: Data Security and Protection Toolkit – NHS tool for assessing data security compliance.
- **Data Centre** – an offsite physical facility housing networked servers and computer systems that process and store information relating to BrisDoc's critical clinical and business systems.
- **Database** – an organised collection of information/data.
- **Encryption** – The means of automating the protection of IT systems, information, and data by making them unreadable without an electronic code from outside influences, e.g. computer viruses, unauthorised access BrisDoc hardware and software.
- **GDPR**: General Data Protection Regulation – UK/EU law governing personal data protection.
- **GP**: General Practitioner – a doctor providing primary care services.
- **HSCN**: Health and Social Care Network – secure network for NHS and social care organisations.
- **IAO**: Information Asset Owner – person responsible for managing specific information assets.
- **ICT**: Information and Communications Technology – systems and tools for storing, processing, and transmitting data.
- **ID**: Identification – usually refers to ID badges or credentials.
- **Identity Access Management**: Processes and tools to ensure the right individuals have appropriate access to systems and data.
- **IGMS**: Information Governance Management System – framework for managing information securely and legally.
- **Information Asset Owner (IAO)**: Person responsible for managing and protecting specific information sets.
- **IT**: Information Technology – technology for storing, processing, and transmitting data.
- **Integrity** – Ensuring that information has not been corrupted, falsely altered, or otherwise changed such that it can no longer be relied upon.
- **LAN**: Local Area Network – network connecting computers within a building or office.
- **Malware** – Software intended to cause harm or disruption to computers or networks. There are many classifications of Malware (Malicious Software) but as a general term it

deals with all forms of viruses, spyware, Trojans, and other software designed with malicious intent.

- **Memory Sticks** – a portable (pocket sized) storage device used to transfer information between computers via the Universal Serial Bus (USB) port.
- **Mobile Device** – These IT devices were designed to be able to provide PC functionality to support working whilst on the move or provide portable PC functionality which can be taken to different locations. Examples include laptops, rugged laptops, tablets, smart phones, etc.
- **MS**: Microsoft – refers to Microsoft products like Teams and Office.
- **Multi-Factor Authentication (MFA)**: Security method requiring two or more verification steps to log in.
- **Network** – Connects IT equipment together to enable the transfer of information. Networks fall into one of these categories:
- ▪ **LAN** – Local Area Network, joining computers and IT equipment in proximity such as an office or building using wires.
- ▪ **WLAN** – Wireless Local Area Network, the same as a LAN but using wireless technology (electronic signals/radio transmissions).
- ▪ **WAN** – Wide Area Network, joining computers or other LANs across a large geographical area.
- **O365 / N365** – Office 365 is a productivity suite of web and desktop applications provided by Microsoft, based on a "cloud" platform.
  BrisDoc operates both and N365 & its own O365 platform.
  a. **N365** – is the NHS version of O365, BrisDoc has limited functionality with this tenant, its primary purpose it to provide all BrisDoc Employees with NHS email addresses and MS Teams access.
  b. **O365 BrisDoc Version** - This version is primary use in the corporate side of BrisDoc and help us overcome the limitations of the N365 License.
  c. **Microsoft Office Suite** – Outlook, Word, Excel, PowerPoint, OneNote, and Access.
  d. **Microsoft Teams** – A collaboration hub of multiple Teams sites that combines voice and video conferencing with instant messaging (Chat and Posts) and document storage, along with other integrated applications.
  e. **Microsoft OneDrive** – A personal drive where personal documents are stored securely in the Cloud to allow easy access from any device, along with secure file sharing. This is an alternative to personal file shares.
  f. **Microsoft Forms** – An application to create surveys, quizzes, polls, and questionnaires; capture submitted data for presentation in the application or for download.
- **NHS**: National Health Service – the publicly funded healthcare system in the UK.
- **PC** – Personal Computer a generic term used to describe most computers designed for use by one person at a time.
- **PID** – Personal Identifiable Data/Information is information about a person which would enable that person's identity to be established by one means or another. This might be detail that would make it easy for someone to identify a person, such as an unusual

surname or isolated Postcode or bits of different information which if taken together could allow the person to be identified. Person identifiable data includes one or more of the following:

- ▪ Name.
- ▪ Postcode.
- ▪ NHS Number or other identifiable number.
- ▪ Date of Birth.
- ▪ Clinical Diagnosis, where this is unusual or rare.
- **Password Manager**: Software that stores and manages passwords securely.
- **Remote Access**: Ability to securely connect to BrisDoc systems from outside the office.
- **Recovery** – Restoration of a system to its desired state following a failure in the operation of the system.
- **Server** – A computer on a network that runs one or more applications/ services (as a host) that can be accessed by other authorised users. This could be a database, file share, mail/printing services, etc.
- **Social Engineering (or Blagging)** – Is where an attacker uses human interaction (social skills) to deceive others to obtain information about an organisation and its information assets including personal data. An attacker may potentially masquerade as a respectable and plausible person claiming bona fide interest in the information concerned e.g. posing as a member of the organisation’s staff.
- **Senior Information Risk Owner (SIRO)**: Executive accountable for managing information risk across the organisation.
- **SFTP**: Secure File Transfer Protocol – a secure way to transfer files over a network.
- **SPAM**: Unsolicited bulk email – often advertising or malicious content.
- **SSLVPN**: Secure Socket Layer Virtual Private Network – encrypted remote access method.
- **Tenant**: A dedicated environment within a cloud platform (e.g., Microsoft 365) for BrisDoc’s data and users.
- **Two-Factor Authentication (2FA)**: A type of MFA using two verification steps, usually password plus code.
- **USB**: Universal Serial Bus – standard for connecting devices to computers.
- **UPS** – Uninterruptable Power Supply, a power supply that typically includes a battery to maintain power in the event of power outage. These can provide power for varying periods of time but are primarily used within BrisDoc to provide protection from damage to servers from fluctuating power input and from short term power loss and resumption of power. The UPS is not for the purposes of business continuity as it will not provide power for a building.
- **User** – Any person that accesses BrisDoc HealthCare Services Systems. This includes, but is not limited to, non-executive Directors, GP’s, organisation employees, consultants, contractors, researchers, trainees, students, and temporary staff.

- **VOIP**: Voice Over Internet Protocol – technology for making phone calls over the internet.

Version Control

Date	Version	Author	Change Details
28/11//2025	1.0	NN	Document created.