Information Security and Cyber Security Policy

Version Control

Reference Number ISCS1	**Version** 1.0	**Status** Final	**Sponsor(s)/Author(s)** J McMullan
Document objectives: Sets out PH's policy on managing threats to Information Security and Cyber Security			
Intended Recipients: All staff			
Group/Persons Consulted: TecSec			
Training/Resource Implications: Induction mandatory training, awareness of policy folder			
Approving Body and Date first approved		Executive Board – ratified 28 May 2026	
Next Review Date		May 2027	

The table below logs the history of the steps in development of the document.

Version	Date	Author	Comment
1.0	July 2012	J McMullan	Written by SIRO as new policy

Table of Contents

---

1. Introduction

Pioneer Healthcare is an independent healthcare provider delivering secondary care services to NHS and private patients across England.

Pioneer Healthcare recognises that information and cyber security are fundamental to the safe delivery of healthcare services, protection of confidential information, maintenance of patient trust, organisational resilience and regulatory compliance.

The organisation is committed to ensuring the confidentiality, integrity and availability of all information assets, whether held electronically, on paper, verbally or in any other format.

This policy establishes the framework through which Pioneer Healthcare manages information security risks, protects sensitive information, safeguards digital infrastructure and responds effectively to cyber threats.

Pioneer Healthcare acknowledges that cyber threats to healthcare organisations continue to evolve rapidly and that robust information security controls are essential to maintaining safe clinical operations and protecting patient data.

2. Purpose

The purpose of this policy is to:

- Protect confidential patient, staff and organisational information;
- Ensure compliance with legal, regulatory and contractual obligations;
- Reduce risks associated with cyber threats and information loss;
- Establish clear responsibilities for information security;
- Promote a culture of cyber awareness and secure working practices;
- Support business continuity and operational resilience;
- Ensure information systems remain secure, reliable and available;
- Maintain public confidence and organisational reputation.

3. Scope

This policy applies to:

- All Pioneer Healthcare employees;
- Directors and senior managers;
- Contractors and agency workers;
- Consultants and clinicians;
- Volunteers and students;
- Third-party suppliers and service providers;
- All systems, devices and networks used for Pioneer Healthcare business;
- Cloud-hosted systems and external platforms;
- Information processed on behalf of NHS organisations.

The policy applies to all forms of information including:

- Electronic records;
- Patient records;
- Emails and messaging systems;
- Paper records;
- Images and recordings;
- Portable media;
- Cloud-based information;
- Backups and archives.

4. Definitions

Term	Definition
Confidential Information	Information that identifies an individual or is commercially sensitive
Cyber Security	Measures used to protect systems, networks and data from cyber attack
Information Asset	Any information, system, application or device holding organisational data
Personal Data	Information relating to an identifiable individual
Special Category Data	Sensitive personal data requiring additional protection under UK GDPR
SIRO	Senior Information Risk Officer
DPO	Data Protection Officer
DSPT	NHS Data Security and Protection Toolkit

5. Legislative and Regulatory Framework

Pioneer Healthcare will comply with all relevant legislation, standards and guidance including:

- UK General Data Protection Regulation (UK GDPR);
- Data Protection Act 2018;
- Human Rights Act 1998;
- Common Law Duty of Confidentiality;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988;
- Privacy and Electronic Communications Regulations (PECR);
- Health and Social Care Act 2008;
- NHS Records Management Code of Practice 2021;
- NHS Data Security and Protection Toolkit requirements;
- Cyber Essentials standards;
- ICO guidance and codes of practice;
- NHS England cyber security guidance;
- Caldicott Principles.

Although Pioneer Healthcare is not an NHS Trust, the organisation is committed to meeting the standards expected of providers delivering NHS-funded healthcare services.

6. Information Security Principles

Pioneer Healthcare will ensure:

6.1 Confidentiality

Information is only accessible to authorised individuals with a legitimate business need.

6.2 Integrity

Information remains accurate, complete and protected from unauthorised alteration.

6.3 Availability

Information and systems remain available when required to support clinical and operational services.

6.4 Accountability

All users are responsible for the secure handling of information.

6.5 Resilience

Systems and services are capable of resisting and recovering from cyber incidents.

---

7. Governance Structure and Responsibilities

7.1 Board of Directors

The Board holds overall accountability for information governance, cyber security and information risk management.

The Board will:

- Receive assurance regarding cyber and information security risks;
- Ensure appropriate resources are allocated;
- Support organisational compliance;
- Review significant incidents and risks.

7.2 Senior Information Risk Officer (SIRO)

The SIRO is responsible for:

- Leading information risk management;
- Overseeing cyber security governance;
- Reviewing significant incidents and breaches;
- Ensuring risk mitigation plans are implemented;
- Reporting major risks to the Board.

7.3 Caldicott Guardian

The Caldicott Guardian oversees:

- Confidentiality of patient information;
- Appropriate information sharing;
- Compliance with Caldicott Principles.

7.4 Data Protection Officer (DPO)

The DPO is responsible for:

- Monitoring data protection compliance;
- Advising on DPIAs;
- Liaising with the ICO;
- Supporting breach investigations.

7.5 Managers

Managers are responsible for:

- Ensuring staff comply with this policy;
- Ensuring local security controls are maintained;
- Supporting staff training;
- Reporting incidents promptly.

7.6 All Staff

All staff are responsible for:

- Protecting information assets;
- Following organisational policies;
- Reporting incidents immediately;
- Maintaining confidentiality;
- Completing mandatory training.

---

8. Information Risk Management

Pioneer Healthcare will maintain a structured information risk management framework.

This includes:

- Information Asset Registers;
- Information risk assessments;
- Data Protection Impact Assessments (DPIAs);
- Cyber risk assessments;
- Supplier assurance reviews;
- Business continuity planning.

Information risks will be reviewed regularly and escalated through governance structures where appropriate.

---

9. Cyber Security Framework

Pioneer Healthcare will implement proportionate technical and organisational security measures including:

- Firewall protection;
- Endpoint protection and anti-malware systems;
- Multi-factor authentication;
- Encryption technologies;
- Secure backups;
- Network monitoring;
- Vulnerability scanning;
- Patch management;
- Access controls;
- Cyber incident response arrangements.

The organisation will work towards and maintain Cyber Essentials standards where appropriate.

---

10. Access Control and Authentication

Access to systems and information will:

- Be role-based;
- Be limited to authorised users only;
- Be regularly reviewed;
- Be removed promptly when staff leave or change roles.

Shared accounts should be avoided wherever possible.

Privileged access accounts must be tightly controlled and monitored.

---

11. Password and Multi-Factor Authentication Standards

All users must:

- Use strong passwords;
- Keep passwords confidential;
- Never share credentials;
- Change compromised passwords immediately.

Multi-factor authentication (MFA) will be implemented for:

- Remote access;
- Administrative accounts;
- Cloud systems where available;
- Sensitive applications.

---

12. Information Asset Management

Pioneer Healthcare will maintain an Information Asset Register identifying:

- Systems;
- Databases;
- Devices;
- Software applications;
- Critical information assets.

Each asset will have an assigned Information Asset Owner.

---

13. Acceptable Use of Systems

Organisational systems must be used responsibly and professionally.

Users must not:

- Access inappropriate or unlawful material;
- Install unauthorised software;
- Circumvent security controls;
- Use systems for unauthorised commercial purposes;
- Share confidential information insecurely.

Limited personal use may be permitted where it:

- Does not interfere with work duties;
- Does not compromise security;
- Does not breach policy or law.

---

14. Remote Working and Mobile Devices

Remote working arrangements must ensure:

- Confidentiality of information;
- Secure internet connections;
- Device encryption;
- Screen locking;
- Safe storage of information.

Devices used remotely must:

- Be password protected;
- Use updated security software;
- Be protected against unauthorised access.

Public Wi-Fi should not be used for accessing sensitive systems unless protected by secure VPN access.

---

15. Bring Your Own Device (BYOD)

Personal devices used for organisational business must:

- Be approved where required;
- Have appropriate security controls;
- Use device encryption;
- Permit remote wipe where necessary.

Pioneer Healthcare reserves the right to restrict or prohibit BYOD access where risks cannot be adequately controlled.

---

16. Email, Internet and Communications Security

Users must:

- Exercise caution when opening emails or attachments;
- Verify suspicious communications;
- Use secure email systems when transferring confidential information;
- Follow organisational email etiquette standards.

Users must not:

- Open suspicious attachments;
- Click unknown links;
- Use unauthorised messaging platforms for confidential information;

- Forward phishing or scam emails.

All suspected phishing emails must be reported immediately.

---

17. Cloud Services and Third-Party Suppliers

Third-party suppliers processing Pioneer Healthcare information must:

- Demonstrate appropriate cyber security standards;
- Comply with UK GDPR requirements;
- Sign appropriate contractual agreements;
- Undergo due diligence assessments.

Cloud services must be approved before use.

Unauthorised cloud storage platforms must not be used for confidential information.

---

18. Data Classification and Handling

Information will be classified according to sensitivity and handled appropriately.

See Appendix B for classification categories.

Users must:

- Store confidential information securely;
- Limit access to authorised individuals;
- Dispose of information securely;
- Transfer information using approved methods.

---

19. Encryption and Secure Transfer

Confidential information transferred electronically must be appropriately protected.

Encryption must be used where:

- Sensitive information is stored on portable devices;
- Information is transferred externally;
- Cloud systems are used.

Approved secure email systems should be used when sharing confidential patient information.

---

20. Records Management and Secure Disposal

Records must be managed in accordance with:

- Legal requirements;
- NHS retention schedules where applicable;
- Organisational procedures.

Information no longer required must be securely disposed of.

Paper records containing confidential information must be shredded or disposed of using approved confidential waste services.

Electronic media must be securely erased or destroyed.

---

21. Malware, Phishing and Cyber Threat Protection

Pioneer Healthcare will maintain measures to:

- Detect malware;
- Prevent ransomware attacks;
- Monitor suspicious activity;
- Protect systems against phishing attempts.

Staff must remain vigilant and report:

- Suspicious emails;
- Unexpected system behaviour;
- Suspected malware;
- Potential cyber attacks.

---

22. Patch Management and Vulnerability Management

Systems and software must:

- Be maintained appropriately;
- Receive security updates promptly;
- Undergo vulnerability assessments where appropriate.

Critical vulnerabilities must be addressed as a priority.

Unsupported software should not be used unless formally risk assessed and approved.

---

23. Backup, Business Continuity and Disaster Recovery

Pioneer Healthcare will maintain:

- Secure backups;
- Disaster recovery arrangements;
- Business continuity plans;
- Recovery testing processes.

Backups must:

- Be protected from unauthorised access;
- Be tested regularly;
- Support restoration of critical services.

---

24. Incident Reporting and Data Breach Management

All actual or suspected information security incidents must be reported immediately.

Incidents include:

- Lost devices;
- Unauthorised disclosure;
- Phishing attacks;
- Malware infections;
- System compromise;
- Ransomware;
- Misdirected emails;
- Data loss.

Serious incidents may require:

- Escalation to the SIRO;
- Notification to the ICO within 72 hours;
- Notification to NHS partners or commissioners;
- External cyber security support.

A formal investigation and lessons learned review will be undertaken following significant incidents.

---

25. Monitoring and Audit

Pioneer Healthcare reserves the right to:

- Monitor use of organisational systems;
- Audit compliance with this policy;
- Investigate suspected misuse.

Monitoring will be proportionate, lawful and conducted in accordance with applicable legislation.

---

26. Training and Awareness

All staff must complete mandatory information governance and cyber security training.

Training will include:

- Data protection;
- Confidentiality;
- Cyber awareness;
- Phishing awareness;
- Incident reporting;
- Safe handling of information.

Additional role-based training may be required.

---

27. Non-Compliance

Failure to comply with this policy may result in:

- Disciplinary action;
- Removal of system access;
- Contractual action;
- Referral to regulatory bodies;
- Civil or criminal proceedings.

---

28. Equality and Diversity

Pioneer Healthcare is committed to ensuring this policy is applied fairly and consistently.

No individual will be discriminated against on the grounds of:

- Age;
- Disability;
- Gender reassignment;
- Marriage and civil partnership;
- Pregnancy and maternity;
- Race;
- Religion or belief;
- Sex;
- Sexual orientation.

---

29. Review

This policy will be reviewed annually or sooner if:

- Legislation changes;
- Significant cyber incidents occur;
- Organisational changes arise;
- National guidance changes.

Appendix A – Named Roles

Role	Post Holder
SIRO	Medical Director – John McMullan
Caldicott Guardian	Medical Director – John McMullan
Data Protection Officer	Chief Executive Officer – Prasad Godbole
Information Governance Lead	Director of Operations – Nicola Salkeld

---

Appendix B – Information Classification Levels

Classification	Description
Public	Information suitable for public release
Internal	Routine operational information
Confidential	Sensitive patient, staff or business information
Highly Confidential	Highly sensitive information requiring enhanced controls

---

Appendix C – Incident Reporting Escalation

Incident Type	Escalation Requirement
Minor incident	Line manager and IG Lead
Potential data breach	DPO and SIRO
Significant cyber attack	Executive escalation and external support
ICO-reportable breach	ICO notification within 72 hours

Policy Approval

This policy is approved and fully endorsed by the Board of Directors of Pioneer Healthcare.

Pioneer Healthcare recognises that effective information security and cyber resilience are essential to the safe delivery of healthcare services and the protection of confidential information.