

Policy/Procedure Name:	Information and Cyber Security Policy
Policy/Procedure Number:	ICT005
Date of Approval:	15 July 2011
Effective Date:	15 July 2011
Revised Date:	August 2026
Review by Date:	September 2029
Policy/Procedure Author:	Head of Technology
Policy/Procedure Owner:	Finance and Resources Director
Management Committee Approved By:	TLT
Governor Committee (where appropriate) Approved By:	n/a
For Action By:	All staff, workers, contractors, volunteers, governors, trustees, agency staff and other authorised users
For Information to:	All staff and authorised users
Approval requested to upload on the Treloar's Website:	Yes ✓
Who is carrying out EIA?	Lorna Woodcroft
Date of EIA?	23 rd October 2025
Have we shown due regard for the 9 protected characteristics within the policy/procedure?	Yes ☐ No ☐
Are all opportunities to promote equality taken within the policy/procedure?	Yes ☐ No ☐
Refer Policy/Procedure to EDI Co-ordinator for further assessment	Yes ☐ No ☐

Aim

The purpose of this policy is to establish the minimum information security requirements that protect the confidentiality, integrity and availability of Treloar's information, systems, services and technology assets.

This policy establishes:

- information security principles and governance requirements
- responsibilities for protecting information and technology assets
- information classification and handling requirements
- physical and digital security controls
- identity and access management controls

- device, network and cloud security requirements
- security monitoring, incident management and reporting requirements
- supplier and third-party security requirements
- Artificial Intelligence security requirements
- assurance, audit and compliance arrangements

Treloar's recognises that information security supports safeguarding, education, care, therapy, health services, workforce management, regulatory compliance, business continuity and organisational resilience. Information security is therefore everyone's responsibility.

Policy Details

This policy applies to all information, systems, services, technology assets, users and third parties processing information on behalf of Treloar's. It establishes the minimum mandatory controls required to protect confidentiality, integrity and availability of information and technology services across the organisation. The requirements of this policy apply regardless of whether information is held electronically, on paper, internally, externally, on-site or remotely.

Key Responsibilities

Treloar Leadership Team - Responsible for:

- providing strategic oversight of information security and cyber security risk
- supporting proportionate investment in security controls
- reviewing significant information security risks and major incidents
- ensuring managers understand mandatory minimum standards

Finance and Resources Director - Responsible for:

- owning this policy
- providing senior oversight of information risk, data protection and freedom of information responsibilities
- supporting escalation of significant security incidents
- coordinating regulatory engagement where required

Data Protection Officer - Responsible for:

- advising on personal data breaches, DPIAs, supplier data protection risks, data subject rights, transparency and lawful processing where information security controls affect personal data

Head of Technology - Responsible for:

- maintaining this policy and aligning it with the wider ICT policy suite
- leading information security governance and security architecture
- supporting Cyber Essentials and wider assurance activity
- coordinating ICT security incident response and supplier security assurance

Computer Services - Responsible for:

- operating day-to-day security controls
- managing user access, devices, endpoint protection, monitoring, alerting, vulnerability management, patching, backup and recovery controls
- supporting investigation of security incidents

Managers and system owners - Responsible for:

- ensuring staff understand security responsibilities relevant to their role
- requesting access only where there is an authorised business need
- supporting local compliance checks, incident reporting and corrective action

All staff and authorised users - Responsible for:

- protecting Treloar information
- using approved systems and devices responsibly
- following ICT policies and procedures

- reporting suspected incidents, inappropriate use, data breaches or security concerns promptly

Use of any system, device, AI tool, cloud service, communication platform or business process does not transfer accountability from the user to the platform or process.

Policy Principles

Scope and application

This policy applies to all Treloar's staff, workers, contractors, volunteers, governors, trustees, agency staff and any other authorised user who creates, accesses, stores, shares, transmits, manages or protects Treloar information or technology assets.

This policy applies to information and systems in any format or location, including paper records, Microsoft 365, Outlook, Teams, SharePoint, OneDrive, Databridge, Nourish, iTrent, Sage, service desk systems, approved cloud services, end-user devices, mobile devices, removable media, network infrastructure, backup systems and other approved organisational systems.

This policy applies whether information is accessed on-site, off-site, remotely, through a managed device, through an approved personal device, through a supplier service or through an approved cloud platform.

Document type and authority level

This document is a governance policy. Requirements in this policy are mandatory where they relate to legal, regulatory, safeguarding, data protection, information security, cyber security, records management, business continuity or organisational risk controls. Guidance language is used only where local professional judgement is required.

Information security principles

Treloar's adopts the following information security principles:

Confidentiality	Information must only be accessed, used or shared by authorised people for authorised purposes
Integrity	Information and systems must be accurate, complete, reliable and protected from unauthorised or accidental alteration
Availability	Information and systems must be available to authorised users when required for legitimate organisational purposes
Accountability	Access, decisions and changes should be attributable to an identifiable user, process or authorised activity where system functionality permits
Least Privilege	Users must only have the access needed for their role and authorised tasks
Defence In Depth	Information must be protected through layered technical, organisational and physical controls
Security By Design	New systems, suppliers, processes and technologies must consider security risks before implementation or material change
Data Protection by Design and Default	Personal data must be protected throughout the lifecycle of the processing activity

Continuous Improvement	Controls must be reviewed and improved in response to risk, incidents, assurance activity and changes in technology or regulation
------------------------	---

Information classification and handling

Important organisational information should be assigned a security classification that reflects its sensitivity, business value and potential impact if disclosed, altered, lost or unavailable.

Classification	Description	Examples
Public	Information approved for unrestricted release	published policies, public website content, general prospectus material
Internal	Routine organisational information intended for authorised Treloar use	internal guidance, routine operational updates, non-sensitive working documents
Confidential	Information that could cause distress, harm, financial loss, reputational impact or operational disruption if disclosed inappropriately	student information, staff information, HR information, finance information, commercially sensitive information
Restricted	Information where disclosure, alteration, loss or unavailability could cause significant safeguarding, legal, regulatory, clinical, security or operational harm	safeguarding records, care or clinical records, security investigations, authentication credentials, privileged access information, high-risk incident evidence

Staff must use approved systems and handling methods appropriate to the classification, sensitivity and purpose of the information. Where classification is unclear, the higher level of protection should be applied until advice is obtained.

Access control and identity management

Treloar's shall operate a least-privilege access model. Access to systems, information, shared locations and administrative functions must be based on authorised business need.

- unique user accounts must be used wherever reasonably practicable
- passwords, passphrases, PINs, authentication prompts and multi-factor authentication methods must not be shared
- multi-factor authentication must be used where implemented or required by Treloar
- access must be approved, changed or removed through authorised joiner, mover and leaver processes
- privileged or administrative access must be limited, controlled and reviewed proportionately to risk
- access to confidential or restricted information must be reviewed where there is a role change, incident, investigation, safeguarding concern, termination of employment or change in business need

Device, endpoint and mobile security

Treloar-owned devices and approved managed devices must be protected using proportionate technical controls. These may include device management, encryption, endpoint protection,

operating system updates, application controls, configuration baselines, remote lock or wipe capability and monitoring where authorised.

Treloar may restrict, suspend or remove access to organisational systems where a device does not meet security requirements, presents a specific security risk or is being used in a way that threatens confidentiality, integrity or availability.

Personal devices used for work purposes must comply with ICT001, ICT002, ICT009 and any approved mobile device or BYOD controls. Organisational information must not be stored outside approved systems unless specifically authorised and protected.

Network, cloud and Microsoft 365 security

Treloar's network, Microsoft 365 environment and approved cloud platforms must be configured and managed to protect organisational information and support safe, secure and reliable working.

- identity and access controls must be applied according to role and risk
- audit logging, alerting and monitoring must be enabled where available and proportionate
- sharing settings must support appropriate access control and prevent unnecessary exposure
- users must not bypass authentication, filtering, monitoring, device security controls or network protections
- approved storage locations must be used for organisational records and working files
- recovery arrangements must be maintained for critical systems and data where reasonably practicable

Physical security and paper records

Paper records and physical media containing internal, confidential or restricted information must be protected from unauthorised access, loss, theft, accidental disclosure or inappropriate disposal.

- confidential and restricted paper records must be stored securely when not in use
- off-site handling of paper records or removable media must be limited to genuine business need and protected proportionately
- paper records must be destroyed securely when no longer required and only in line with ICT003 Retention of Records Policy
- loss or suspected loss of paper records, equipment or removable media must be reported promptly

Removable media and portable storage

Removable media and portable storage must not be used for Treloar information unless there is a genuine business need and suitable security controls are in place.

- use must be authorised where required by local procedure or risk
- confidential or restricted information must be encrypted using an approved method where removal from approved systems is unavoidable
- lost, damaged or unneeded removable media must be reported or returned to Computer Services for secure disposal or sanitisation
- removable media must not be used to bypass approved file storage, sharing, archival or retention controls

Data protection, records and information governance

Information security controls must support the requirements of ICT002 Data Protection Policy, ICT003 Retention of Records Policy, ICT009 Electronic Communications and Information Sharing Policy and ICT010 Data Quality and Records Assurance Policy.

Personal data, special category data, safeguarding information, care records, clinical information, staff information, financial information and confidential organisational information

must only be accessed, used, shared, retained or destroyed where there is an authorised, necessary and lawful purpose.

Technical retention, backup, recovery, logging and platform housekeeping controls do not determine the retention period of organisational records. Official records must be retained, archived or destroyed in accordance with ICT003.

Confidential waste and secure disposal

All staff are responsible for ensuring that confidential information is disposed of securely when it is no longer required. This applies to paper records, printed documents, notes, removable media and any other material containing personal, confidential or commercially sensitive information.

- Personal information and confidential records must not be placed in general waste or recycling bins unless all confidential information has first been securely removed or destroyed.
- Paper records containing personal information, special category data, safeguarding information, staff information, student information or sensitive policy information must be shredded or placed in an approved confidential waste container prior to disposal.
- Draft documents, working notes, printed reports and photocopies containing confidential information must be disposed of using confidential waste arrangements when no longer required.
- Staff must take reasonable steps to prevent unauthorised access to confidential waste awaiting collection or destruction. Confidential waste should not be left unattended in public or unsecured areas.
- Removable storage devices, including USB memory sticks, external hard drives, mobile phones and other electronic media containing Treloar's information, must not be discarded through normal waste streams. Devices that are no longer required or have become damaged must be returned to the Tech Hub for secure data removal and sanitisation.
- Where confidential documents are produced or used off-site, staff must ensure they are either returned to Treloar's for secure disposal or destroyed using an equivalent secure method.
- The destruction of records must be carried out in accordance with ICT003 Retention of Records Policy and any applicable departmental retention requirements.

Computer Services donate retired stock to WEEE registered charities, and also use on-site WEEE bins in the event those charities have no requirement for the hardware.

Failure to dispose of confidential information securely may constitute a data breach and must be reported immediately through the IRIS system in accordance with this policy.

Artificial Intelligence and emerging technologies

AI, automation, transcription, analytics and emerging technologies must be used in accordance with ICT002, ICT012A, ICT012B, ICT013 and any approved governance process.

Staff must not enter the following into unapproved external AI tools or unapproved automated services unless the tool, use case and safeguards have been approved:

- personal data
- student information
- care records
- clinical information
- safeguarding information
- employee information
- financial information
- confidential information
- commercially sensitive information

- photographs or recordings of students or staff without express and appropriate approval
- any information classified as Internal, Confidential or Restricted where disclosure has not been authorised

Supplier security standards and third-party expectations

Supplier assurance activity, including questionnaires, security evidence, contract checks, DPIAs, Data Processing Agreements and periodic review, is managed through the relevant assurance, procurement, data protection or contract ownership process rather than being fully defined in this policy.

From September 1st 2026, supplier security due diligence shall be completed by the Head of Technology (or a designated member of his team) before onboarding any supplier processing Treloar information and shall be reviewed at least every three years or sooner where risk changes materially.

Cyber Essentials, ISO27001 or equivalent assurance may be used as evidence where appropriate, but the required assurance will depend on the risk, role and sensitivity of the supplier relationship.

- secure deletion, return of data and exit arrangements at the end of the service
- sub-processor, subcontractor and onward-transfer controls where relevant
- backup, recovery, resilience and service continuity arrangements where relevant
- incident notification and cooperation with security or data protection investigations
- confidentiality, staff screening or contractual confidentiality commitments where relevant
- access control, privileged access and support access arrangements
- information security arrangements appropriate to the service and risk
- UK GDPR, Data Protection Act and processor obligations where personal data is processed

Where suppliers store, access, transmit, process or support Treloar information, Treloar's expects appropriate controls covering:

Supplier security expectations must be proportionate to the nature of the service, the sensitivity of the information, the level of access provided and the potential impact on safeguarding, care, education, business continuity, data protection or cyber security.

Treloar's will only use suppliers, processors, support providers and third parties that can demonstrate appropriate organisational, technical and contractual controls to protect information and support legal, regulatory and operational requirements.

Security monitoring, audit and access to communications

Treloar may monitor technology systems, communications, audit logs, network activity, access activity and security alerts where necessary and proportionate to support safeguarding, information security, prevention and detection of misuse, business continuity, regulatory compliance, legal obligations or incident investigation.

Microsoft 365 audit, security and compliance logs may be used to support information security, safeguarding, cyber security, incident investigation, compliance monitoring, data protection obligations and organisational assurance activities.

Access to audit and security logging information must be restricted to authorised staff and used only for approved purposes.

Security monitoring, alerting and audit evidence should be reviewed regularly by Computer Services and escalated where a safeguarding, data protection, cyber security or operational concern is identified.

Security incidents, personal data breaches and reporting

All security incidents must be reported through IRIS. Incidents involving technology, cyber security or personal data must additionally be reported to Computer Services as soon as practicable.

Where an incident may involve personal data, the Data Protection Officer must be involved so that notification duties and data subject communication duties can be assessed. Where safeguarding, care, clinical, HR, legal or regulatory risks are involved, the relevant professional lead must also be informed.

Service desk records, support tickets, incident records and technical investigation records form part of Treloar's operational assurance framework and must be retained in accordance with ICT003 Retention of Records Policy and the applicable RoPA entry.

Where service desk records become part of a complaint, safeguarding matter, HR matter, security investigation, legal hold, regulatory investigation or other official record, retention requirements for that record category shall take precedence.

Security incidents must be recorded, assessed, contained and reviewed proportionately. Lessons learned should be used to improve controls, guidance, training and assurance activity.

Business continuity, backup and recovery

Treloar shall maintain proportionate backup, recovery and technology continuity arrangements for critical systems and information. Recovery priorities should reflect safeguarding, care, clinical, education, operational, legal, financial and regulatory need.

- Critical systems and data should have defined backup or recovery arrangements where reasonably practicable
- Recovery arrangements should be reviewed or tested proportionately to risk and business need
- Cyber incident recovery must consider containment, restoration, validation, communications and lessons learned
- Backup and recovery controls do not replace official record retention requirements under ICT003

Exceptions and risk acceptance

Exceptions to this policy must be justified, proportionate, time-limited where appropriate and approved by the relevant policy owner, risk owner or senior decision-maker. Exceptions involving personal data, confidential or restricted information, safeguarding, clinical, care, HR, finance, cyber security or supplier risk must be escalated before implementation where practicable.

Where an exception is approved, compensating controls should be recorded where appropriate.

Non-compliance and policy breach

Failure to comply with this policy may result in access being restricted or removed, management action, investigation under relevant organisational procedures and, where appropriate, disciplinary action. Serious breaches involving personal data, safeguarding information, confidential information, deliberate misuse, unauthorised access, cyber security incidents or attempts to bypass controls may require reporting under data protection, safeguarding, contractual, legal or regulatory requirements.

Implications of Policy/Procedure

Training and Communication Requirement

	Action	Responsibility
1	Ensure that all managers, employees and authorised users have access to this policy and related procedures.	Treloar Leadership Team

2	Train relevant staff in implementation of this policy and related procedures.	Head of HR / Training Manager
3	Ensure new employees, staff and authorised users are made aware of the policy and know where to access it.	Training Manager
4	Ensure staff understand their responsibilities and receive any required role-specific guidance.	All Managers
5	Maintain technical guidance, operational standards and security controls supporting this policy.	Head of Technology / Computer Services

Inclusive Communications

If you require this document in an alternative format, such as large print, audio description or a colour background, please contact Jo Cox at jo.cox@treloar.org.uk.

Training

Treloar's will provide appropriate awareness and guidance covering information security, cyber security, acceptable use, data protection, password management, multi-factor authentication, phishing, social engineering, AI risks, safe sharing, approved systems, incident reporting and confidentiality.

All users are expected to maintain an appropriate understanding of information security risks and responsibilities relevant to their role.

Policy in a Box

What are staff agreeing to?

- Protect Treloar's information, systems, devices and services according to their sensitivity and business purpose.
- Use approved systems, devices and security controls.
- Follow information security, cyber security and data protection requirements.

Staff must not:

- Share passwords, authentication methods or access credentials.
- Bypass security controls, monitoring, filtering or access restrictions.
- Store or process confidential information in unapproved systems or services.
- Upload personal, safeguarding, care, clinical, staff or financial information into unapproved AI tools.

Staff are accountable for:

- The protection of information they access, create, store or share.
- Reporting security incidents, data breaches, suspicious activity or policy breaches promptly.
- Using organisational systems and devices securely and responsibly.

Staff should help Treloar's:

- Protect students, staff, systems and information from cyber threats.
- Maintain confidentiality, integrity and availability of information.
- Support safeguarding, business continuity and regulatory compliance.

Practical Examples of Acceptable and Unacceptable Use

Access and accounts

Acceptable

- using your own account to access systems
- using MFA when prompted
- reporting unexpected sign-in prompts or suspected account compromise

Not Acceptable

- sharing passwords or MFA prompts
- using another person's account
- retaining access after a role change where it is no longer required

Information sharing

Acceptable

- checking recipients, links and permissions before sharing
- using approved secure sending methods for confidential information
- sharing only the minimum information needed

Not Acceptable

- sending confidential information to personal email without approval
- using open links where restricted access is required
- forwarding restricted information without authority

Devices and storage

Acceptable

- using approved managed devices where required
- saving organisational records in approved locations
- reporting lost devices promptly

Not Acceptable

- storing organisational information in personal cloud storage
- bypassing device security controls
- using unencrypted removable media for confidential information

AI and emerging technology

Acceptable

- using approved AI tools in line with policy
- reviewing AI outputs before relying on them
- sanitising information only where the user can verify it is safe

Not Acceptable

- entering confidential, safeguarding, care, clinical, staff or financial information into unapproved external AI tools
- relying on AI outputs without review
- using AI to bypass approved governance controls

Monitoring and Review

This policy must be reviewed annually or earlier where legislation, regulation, systems, security threats, regulatory expectations, cyber security frameworks, assurance findings, significant incidents, supplier arrangements or organisational needs change.

Assurance evidence

- Cyber Essentials assessment and remediation evidence

- Security incident and near-miss reports
- Personal data breach logs and lessons learned
- access reviews for critical systems or privileged accounts
- vulnerability, patching and security posture reviews where available
- backup and recovery checks or test evidence
- supplier security and data protection due diligence records
- audit logs, monitoring alerts, phishing reports and malware reports where relevant
- security awareness or training completion evidence
- internal audit, external audit, regulatory or inspection findings where relevant
- supplier review, procurement or contract-owner assurance records where relevant
- Cyber Essentials, ISO27001 or equivalent supplier assurance evidence where relevant to risk
- Supplier Data Processing Agreements, security schedules or contract security clauses where relevant
- supplier security questionnaires or due diligence evidence where relevant

Links to other related policies, procedures or documents (internal)

- ICT001 - Technology Acceptable Use and Access Policy
- ICT002 - Data Protection Policy
- ICT003 - Retention of Records Policy
- ICT009 - Electronic Communications and Information Sharing Policy
- ICT010 - Data Quality and Records Assurance Policy
- ICT012A - Artificial Intelligence Policy (Staff)
- ICT012B - Student Academic Integrity, Originality and Artificial Intelligence Policy
- ICT013 - Recording, Transcription and Meeting Policy
- Cyber Essentials and ICT operational standards where approved
- Business continuity, safeguarding, HR, finance, procurement and clinical procedures where relevant

Further sources of information (external)

- Information Commissioner's Office guidance on security and personal data breaches
- National Cyber Security Centre guidance and Cyber Essentials requirements
- UK GDPR and Data Protection Act 2018
- Relevant sector cyber security, safeguarding, education, health and social care guidance where applicable

Revision History

Page/para-No.	Brief description of the change(s)	Change made by	Date
All	Clean rebuilt standardised draft aligned to wider ICT policy suite	Head of Technology	August 2026

Equality Impact Assessment (EIA) - Stage 1

Name of Policy / Function/Decision	As per cover sheet
Name of Assessor / Author / Lead	[Insert name / role]
Start Date	[Insert name / role]
This EIA is being undertaken because it is:	Policy review and update.

Does the policy affect employees, students or other stakeholder groups? Could the impact be significant to that group of people?	Y / N
Is it a major policy with a significant effect on how our core business is delivered?	Y / N
Does it involve a significant commitment of resources?	Y / N
Does it relate to an area where there are known inequalities?	Y / N
Have we shown due regard for the 9 protected characteristics within the policy/procedure/decision?	Yes ☐ No ☐
Are all opportunities to promote equality taken within the policy/procedure/decision?	Yes ☐ No ☐
Have we stated how we will monitor the implementation and impact of this policy/decision?	Yes ☐ No ☐
Date of Screening	[Insert]
Approval by EDI	[Insert]
Refer Policy/Procedure to EDI Co-ordinator for further Stage 2 Assessment (if required)	Yes ☐ No ☐