

## ICT SECURITY POLICY

### 1. Purpose

The ICT systems and services of the Two Counties Trust (“the Trust”) form a vital element of operations, and as such must be protected as far as possible from any form of disruption or interruption to service. It is therefore essential that the availability, integrity and confidentiality of the ICT systems and data are maintained at a level that is appropriate for the Trust and Schools (the organisation) needs. This Policy sets out everyone’s responsibility to ensure the ICT system and ICT equipment remain secure.

### 2. Scope

The Trust recognises that threats to systems may arise both internally and externally, and that malicious actors may target employees to gain systems access. The provisions in this policy apply to mitigate the risk posed by threats both inside and outside of the Trust network control.

This Policy covers all employees and users of ICT who have control over, or who use, or support the Trust’s ICT systems or data. Other relevant documents are the Staff Acceptable Use Policy (Appendix 3).

For the purposes of this Policy, an ICT system means any device used for automatic storage and the processing of data.

### 3. Policy Principles

The ICT Security Policy includes the Cyber Security Policy (Appendix 1) and the requirements of the current legislation relating to the use of ICT systems, which comprise principally of:

- GDPR and Data Protection Act 2018
- Computer Misuse Act 1990
- Copyright, Design and Patents Act 1988

It is important that all users are aware that any infringement of the provisions of this legislation may result in disciplinary, civil and/or criminal action. Summary information relating to the legislation set out above is found in Appendix 2. In addition to this policy, the Trust’s Data Protection Policy provides further guidance.

### 4. Policy Elements

#### 4.1 Trust ICT Management

Trust ICT assets and services are controlled by a centralised team. The Trust ICT Team are responsible for the secure running of the Trust systems and services, and take all appropriate steps to ensure the confidentiality, availability, and integrity of these at all times.

Trust ICT assets are managed via a devolved asset control register, with Technical Managers maintaining the register of assets per school, and Trust central assets maintained separately. All hardware issued to end users should be traceable and end users are accountable for the condition of the equipment issued to them.

Systems access is granted by the ICT Team on the principle of least privilege, meaning that only the access required for a user to fulfil their role will be applied to a user account. This is reflected in the privileges assigned to the user object within Active Directory and Office 365. Any privilege change or escalation requires authorisation and should be recorded as a “Request For Access” (RFA) via the ticketing system. This RFA will record the reason for the request, and authorisation from the management of the requestor.

User rights are granted and rescinded in a timely manner on receipt of a status change update from line management or the Human Resources department. This, along with the recovery of allocated ICT assets, forms a key structure of the leaver process.

#### 4.1 Legitimate Use

It is the responsibility of each school to determine the appropriate level of access to the ICT systems, including the Microsoft products, VPN access, the School's MIS system and other software packages, as well as access to shared data resources such as local file servers and online collaborative resources such as Teams and SharePoint.

Requests to the ICT Technical Manager should set out the appropriate level of access to the School's ICT systems before a new member of staff starts work or if a current member of staff changes their role. In addition, HR must inform the ICT Technical Manager when a member of staff leaves employment so that access to the ICT system can be removed when employment ceases. As with central ICT requirements, all RFAs should be recorded via the ticketing system, along with authorisation and any notes about required duration of elevation.

Responsibility for authorisation to the ICT systems lies with the ICT Technical Manager. In all cases, the ICT Technical Manager will be guided on authorisation requirements by the roles laid out by the school management structure and will authorise or deny on a case by case basis. Should there be any uncertainty about the suitability of a level of access this should be escalated to the Central ICT Trust management team and reviewed by the Head of ICT in conjunction with key stakeholders.

Any attempt, or complicity in an attempt, to circumvent the authorisation process for access permissions is a disciplinary offence, as is using the ICT facilities provided to in any way break the law. Examples of such breaches may include (but are not limited to):

- disclosing access credentials for information or services
- obtaining and using another user's details to access information or services
- making, distributing, or using unlicensed software or data
- making or sending threatening, offensive, or harassing materials
- creating, possessing, or distributing obscene material
- unauthorised private use of Trust's computer facilities.

#### 4.2 Use of computer equipment and virus / malware protection

Any computer equipment used to access Trust ICT information or services must be sanctioned by the ICT Management structure as laid out above, and its authorisation recorded in the ICT Asset Register. The process of authorisation must include determining that security software fit-for-purpose is present on the computer equipment. This includes, but may not be limited to, anti-virus endpoint protection, a local firewall, and internet filtering software.

The following conditions are laid out for authorisation:

- only authorised personnel will have access to computer equipment
- only authorised software may be used on any computer equipment
- only software that is used for organisational or educational applications may be used
- no software may be brought onto or taken from the premises without prior authorisation from the ICT Technical Manager.
- before new software is introduced to the network it must be checked and authorised by the ICT Technical Manager.
- unauthorised access to the computer facility, unauthorised copying and/or removal of computer equipment/software, and any attempt to circumvent the software protections deployed by the Trust may result in disciplinary action.

#### 4.3 General security considerations

##### 4.3.1 Backup and recovery

The ICT Team ensure that backups of all ICT services and systems are taken regularly, and that checks are made to confirm the validity of the backup and restore process. This forms a component of the Disaster Recovery and Business Continuity policy, and the full process can be found therein.

### 4.3.2 Monitoring

The Trust will not generally engage in systematic monitoring and recording activities. However, it reserves the right to do so where there is reason to believe that misuse of its information assets or computing facilities is occurring. The Headteachers, Trust Executive and Network Managers reserve the right to monitor all e-mail/internet activity by staff members for the purposes of ensuring compliance with our policies and procedures and of ensuring compliance with the relevant regulatory requirements. Information acquired through such monitoring may be used as evidence in disciplinary proceedings.

Issues discovered via monitoring software that relate to members of staff are immediately reported to the Headteacher or School Safeguarding Lead, or in their absence, their Deputy. Unless requested by the Headteacher / Executive of the Trust, the Head of ICT will take no further steps regarding staff incidents. Should a matter arise that directly involves the Headteacher's / CEO's own use of the system, the matter will be referred by the Head of ICT to the Chair of Governors / Trustees as appropriate.

### 4.4.3 Firewalls and filtering

Regular procedures are in place for the Head of ICT and/or the ICT Technical Managers to check the network for 'unauthorised' files. The ICT Team will ensure that an adequate firewall and internet content filtering are employed to restrict external access and activity to the Trust / School ICT network and to protect the internet connection. The Head of ICT and ICT Technical Managers will always ensure that an adequate email and filtering security software is in place to protect the Trust systems from obvious threats, however there is also a degree of personal responsibility to use the systems within the proscribed limits.

### 4.4.4 Data protection

All data within this policy will be processed in line with the requirements and protections set out in the General Data Protection Regulation (GDPR) and the UK-GDPR post-Brexit transition.

## Limitations of this Policy

While every endeavour is made to secure the ICT systems, the nature of exploits and malicious actors is such that it is possible a route may be found to breach the security of the systems. In this case, and ICT Cyber security incident is declared, and the Incident Management process invoked.

## Document management

Version:	Draft
Author:	Rich Minshaw
Date:	22 <sup>nd</sup> October 2020
Review cycle:	Biennial
Next review due:	November 2022
Policy owner	Head Of ICT, Two Counties Trust
Approving body:	Board of Trustees
Changes in this version:	Reformatting 4.1 RFA process added Role titles changed



## ICT CYBER SECURITY POLICY

### 1. Purpose

This Cyber Security Policy outlines the Trust's guidelines and provisions for preserving the security of data and the technology infrastructure against a cyber-attack.

The more we rely on technology to collect, store, and manage information, the more vulnerable the organisation is to severe security breaches. Human errors, hacker attacks and system malfunctions not only cause great financial damage but also affect business continuity, compromise our GDPR compliance and can adversely affect our reputation.

For this reason, the Trust has implemented a number of security measures and instructions to help mitigate security risks.

### 2. Scope

This policy applies to all employees, contractors, volunteers, and anyone who has permanent or temporary access to systems and hardware.

### 3. Policy Principles

All measures laid out herein are designed to mitigate the effects of cyber threats on:

- The ability of the Trust to deliver services to schools
- The ability of schools to fulfil their teaching and learning responsibilities
- The security and integrity of confidential information, such as:
  - Personal information on students, carers, staff, teachers etc.
  - Unpublished financial information
  - Intellectual property

There is an obligation on all staff within the trust to ensure data and systems are protected in line with the provisions laid out in this policy.

### 4. Policy Elements

#### 4.1 Device management and protection

When staff use their digital devices to access systemic information, such as email or files, they introduce risk to the security of the systems. We therefore require all staff to maintain security on devices used to access such systems by adhering to the following conditions:

- Ensure all devices are secured with a password, PIN, or biometric access process
- Ensure the presence of Trust approved anti-malware (including virus) software on any device
- Always ensure the physical security of devices (e.g. not left on display in a car)
- Only use secure networks to connect to Trust services (e.g. using a VPN if on public Wi-Fi)
- Never disclose or share passwords

Staff should never share or loan their devices; any loss or new requirement should be raised with the ICT Team.

Individuals will receive this policy on joining the Trust and should request clarification on any points they do not sufficiently understand.

## 4.2 Safe use of email

Malicious email is the primary vector of ingress to compromised networks. Therefore, good email discipline and hygiene should be maintained around the use of the Trust's email systems and facility.

Good practises include (but are not limited to):

- Be suspicious of any email with an attachment or which includes links
- Verify the sender is as expected, and any attachment is also expected
- Check links are spelled correctly, and do not hide their true destination (hovering over link text should show the actual target)
- Never open any attachment, or click on any link, of which you are unsure
- Be wary of any email saying a file has been shared with you. Confirm this (verbally if possible) with the sender of the email
- Be wary of an email which says it contains a voicemail. Confirm this with ICT before clicking links or opening attachments

If a staff member is not sure that an email they received is safe, they must refer this to the ICT Department. Suspicious emails should never be forwarded as this can spread a virus.

## 4.3 Authentication management (passwords)

Authentication integrity is a key component of the security of ICT Systems. This includes (but is not limited to) passwords, PIN codes, passphrases, biometric data and cryptographic certificates. In **all** instances these should be treated as highly confidential.

Strong discipline is encouraged when choosing authentication security. Wherever possible multi-factor authentication should be utilised to mitigate the risk of any one credential being compromised.

Passwords, PINs and passphrases should be as secure as possible, and should be memorable so as not to require the user to store this information in an accessible form anywhere.

Password length is a key to good security. For example:

“This is my passphrase and I remember it every day” is substantially more secure than “4^jsyR&f”, due to the length as well as being easy to remember.

## 4.4 Secure data transfer

Transferring data introduces security risk. Staff must:

- Avoid transferring sensitive data (e.g. pupil information, reports or marking sheets) to other devices or accounts unless necessary
- Only share confidential data over the Trust's network (including VPN) and not over public Wi-Fi
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies
- Ensure any email attachments containing personal or confidential data are password protected and ensure that the password to open an attachment is not included in the e-mail (ideally sent via a second channel such as SMS)
- Report scams, privacy breaches and hacking attempts.

In all cases the ICT Team will offer support if requested.

## 4.5 Additional measures

The ICT Team must be made aware of any perceived threat, suspicious activity, or phishing attack. This should be via the usual channels but should be flagged as a cybersecurity concern to ensure appropriate escalation.

The following behaviours are strongly encouraged:

- PCs and Laptops should **always** be locked when left unattended, and the screen turned off
- Report to ICT the presence of any discovered, unexpected, or unexplainable ICT hardware
- Report to ICT any perception of a weakness in the Trust's cybersecurity
- Avoidance of non-work-related web activity on Trust networks, even during breaks

The ICT Team will **always** respond to cybersecurity threats, information or risks urgently, with a pre-defined escalation route being observed.

It is incumbent on the ICT Team to architect services and systems for security, including:

- Firewalls, VPNs, filtering, monitoring and ACL management solutions
- Regular training and briefing notes about new threats and horizon risks
- Responding to any reported cybersecurity incident urgently

#### 4. Policy breaches

It is expected that all employees follow this policy. Any breach of this policy will be treated extremely seriously and may lead to disciplinary proceedings.

#### Limitations of this Policy

While every endeavour is made to secure the ICT systems, the nature of exploits and malicious actors is such that it is possible a route may be found to breach the security of the systems. In this case, an ICT Cyber security incident is declared, and the Incident Management process invoked.

#### Document management

Version:	Draft
Author:	Rich Minshaw
Date:	12 <sup>th</sup> November 2020
Review cycle:	Biennial
Next review due:	November 2022
Policy owner	Head Of ICT, Two Counties Trust
Approving body:	Board of Trustees
Changes in this version:	Reformatting Clarity of phrasing

## Appendix 2 - The Legislation

### 1. Introduction

1.1 A failure to comply with the provisions of the following Acts will be regarded as a breach of policy and may be treated in certain circumstances as gross misconduct and may also result in civil or criminal proceedings being taken.

1.2 In the case of the Data Protection Act, failure to comply with the provisions of the prevailing Act and any subsequent legislation and regulations relating to the use of personal data may result in prosecution by the Information Commissioners Office.

### 2. Data Protection Acts 1984 & 1998, 2018 and General Data Protection Regulations 2018

2.1 It is important that all users of personal data are aware of the requirements of the GDPR Regulations and the limitations on the storage and disclosure of information. All processing of personal data must comply with the eight enforceable principles of good practice. Data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant, and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with the data subject's rights
- secure
- not transferred to other countries without adequate protection and reason.

Please refer to the Data Protection policy.

### 3. Computer Misuse Act 1990

3.1 Under the Computer Misuse Act 1990 the following are criminal offences, if undertaken intentionally:

- Unauthorised access to a computer system or data
- Unauthorised access preparatory to another criminal action
- Unauthorised modification of a computer system or data.

3.1 All users must be aware that deliberate unauthorised use, alteration, or interference with a computer system or its software or data, whether proprietary or written 'in house' will be regarded as a breach of Trust policy and may result in disciplinary action and that in some circumstances such a breach may also be a criminal offence.

### 4. Copyright, Design and Patents Act 1988

4.1.1 The Copyright, Design and Patents Act 1988 provides the legal basis for the protection of intellectual property. Intellectual property covers computer programs and data.

4.2 Where computer programs and data are obtained from an external source, they remain the property of the originator. The Trust's permission to use the programs or data will be governed by a formal agreement such as a licence.

4.3 All copying of software is forbidden under the Act unless it is in accordance with the provisions of the Act and in compliance with the terms and conditions of the respective licence.

## Appendix 3 Staff Acceptable Use Policy

### 1. Introduction

- 1.1 ICT and related technologies such as e-mail, the Internet and mobile devices are an expected part of our daily working life
- 1.2 This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT
- 1.3 All staff must always adhere to this policy
- 1.4 Staff should be aware that a breach of this acceptable use policy may result in disciplinary proceedings.

### 2. Expectations of staff

- To only use work email/Internet/Intranet and any related technologies for professional purposes
- To limit internet for personal use to out of working time and to breaks and lunchtime
- To comply with the ICT system security
- To keep passwords secure
- To ensure that personal details cannot be accessed by those not authorised to have them
- All electronic communications with pupils and staff are compatible with professional responsibilities
- Personal details, such as mobile phone number and personal email address must not be disclosed to students
- All personal data is to be kept secure and used appropriately, whether on or off the premises
- No hardware or software will be installed without the permission of the ICT Department
- Any material that could be considered offensive, illegal or discriminatory will not be browsed for, downloaded, uploaded or distributed
- Personal devices must not be used to record images of students nor should any images of students be downloaded to personal devices
- To accept that use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Headteacher and / or a member of the Trust's Executive Team
- To adhere to e-safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the Trust community
- To respect copyright and intellectual property rights
- All online activity, both in Trust and outside Trust, will not bring the professional role for which staff are employed into disrepute
- Not to permit any current pupil of any age or any ex-pupil of the Trust under the age of 21 as a friend, follower, subscriber or similar on any personal social media account, including any form of on-line gaming
- To only use sanctioned social media accounts for communicating official Trust business or news.

Signed:

Date:

Print name: