THE TWO COUNTIES TRUST

ICT CYBER SECURITY POLICY

Date of issue: 29/04/2021

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    - Unpublished financial information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, as per the ICT Hardware Issuance policy (section 4.1). This also applies if it is suspected that passwords or other credentials have been compromised.

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. It is, however, necessary (e.g., to exam boards). As such, 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

5. 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, and ICT Cyber security incident is declared, and the Incident Management process invoked.