INVICTUS

Education Trust

Cyber-Security Policy

Document Control and Version Control

DOCUMENT CONTROL	
POLICY TITLE:	Cyber Security Policy
POLICY AUTHOR:	Daniel Elwell, Head of Digital Transformation
VERSION NUMBER:	V 2.0
DATE APPROVED:	13.10.2026
DATE EFFECTIVE:	14.10.2026
DATE DUE FOR REVIEW:	October 2027
POLICY STATUS:	Non-statutory policy
POLICY TYPE:	Trust wide
REQUIRED TO PUBLISH:	No
POLICY LEAD:	Daniel Elwell, Head of Digital Transformation
APPROVAL LEVEL:	Executive Team

VERSION CONTROL			
VERSION	**AUTHOR**	**DATE**	**CHANGES**
V 1.0	DE	07.05.2025	New policy
V 1.1	D. Samrai, Head of Innovation	17.06.2026	Policy updated to reflect emerging phishing threats, including the use of AI-generated content to increase the sophistication of attacks.
V 2.0 (this document)	D Elwell, Head of Digital Transformation	Sept 2026	Cyber Security Policy and Anti-Phishing Policy combined into a single policy, to reduce policy duplication and give staff one point of reference for cyber security and phishing

Invictus Education Trust
Cyber Security Policy

Contents

1. Our Mission, Vision and Values 4
2. Introduction, Purpose and Scope 4
3. Abiding by this Policy 4
4. Security Standards and Frameworks 4
5. Our Responsibilities to You 4
6. Our Devices 5
7. Access Control and Identity 5
7.1 Your Account 5
7.2 Multi-Factor Authentication (MFA) 5
7.3 Geographic Access Restrictions 5
7.4 Privileged and Administrative Access 6
8. Phishing and Social Engineering 6
8.1 What to Look For 6
8.2 What to Do 6
8.3 Reporting is Encouraged 6
8.4 Simulated Phishing Campaigns 6
8.5 Reducing Our Exposure 7
9. Cyber Incident Response 7
9.1 Your Immediate Responsibilities 7
9.2 How Incidents are Classified and Managed 7
9.3 Legal Reporting Obligations 8
10. Contact Information 8
11. Compliance 8
12. Glossary of Terms 8
13. Parental Impact Assessment 8

1. Our Mission, Vision and Values

Mission

'Excellence every day, unlimited ambition and transforming lives'

Vision

'To create a community of inclusive schools where people choose to learn with us, work with us and belong with us, so that everyone succeeds'

Values

- Respect
- Resilience
- Relationships

2. Introduction, Purpose and Scope

Invictus Education Trust is committed to protecting its people, data, and digital systems from cyber threats, including phishing and other forms of social engineering. This policy sets out the responsibilities of everyone who uses trust-owned devices or systems - including all staff across all of our schools. Cyber security is not just an IT concern. Every member of staff plays a role in keeping our systems, our pupils' data, and our schools safe.

This policy should be read alongside the Trust's Data Protection Policy, Information Security Policy, BYOD Policy, and Acceptable Use Policy.

This policy is in line with Invictus Education Trust's mission, vision, and values. If you have any questions about this policy, please consult the policy lead listed above, or your headteacher.

3. Abiding by this Policy

All staff are expected to comply with this policy. Violating this policy may result in disciplinary action, up to and including dismissal, in line with the Trust's disciplinary procedures. Where a breach constitutes a criminal offence - for example, unauthorised access to systems or deliberate data destruction - it may be referred to the relevant authorities. Employees affected by this policy are expected to read and follow it, directing any questions to the policy lead.

4. Security Standards and Frameworks

The Trust aligns its cyber security approach with nationally recognised standards. Our baseline is the NCSC Cyber Essentials framework, which defines five foundational controls: firewalls, secure configuration, user access control, malware protection, and patch management. We also draw on the NCSC's 10 Steps to Cyber Security guidance for broader organisational practice.

Invictus Education Trust adopts a multi-layered defence against phishing which incorporates a combination of technological, process, and people-based approaches. By widening our defences, we can improve our resilience against phishing without disrupting the productivity of our students and staff, and create multiple opportunities to detect an attack and stop it before it causes harm. Our phishing defences (set out in Section 8) are built around four areas:

- Making it difficult for attackers to reach our users
- Helping users identify and report suspected phishing emails
- Protecting our organisation from the effects of undetected phishing emails
- Responding quickly to incidents

5. Our Responsibilities to You

The Digital team will:

- Maintain secure, well-managed devices and infrastructure, configured in line with Cyber Essentials standards
- Provide a Company Store with approved applications you can install safely
- Ensure all devices are protected with up-to-date antivirus and endpoint protection software
- Apply critical security patches to managed devices within defined timeframes
- Operate the Central Services Helpdesk so you have a clear route to report concerns or request support
- Ensure all trust systems benefit from firewalls, web filtering, and encrypted storage

- Filter or block phishing emails before they reach users, using techniques including IP address, domain name and email address block/welcome lists, public spam and open relay block lists, attachment-type filtering, and malware detection, and by honouring the anti-spoofing policies of senders' domains
- Apply anti-spoofing controls (such as DMARC, SPF and DKIM) to make it harder for email from our own domains to be spoofed
- Maintain technical security monitoring capability, including proactive monitoring against known threats, and keep this capability up to date
- Deliver regular training and guidance on recognising and responding to cyber threats, including phishing
- Review this policy annually and update it as the threat landscape changes

6. Our Devices

All staff have been issued a trust laptop as part of our digital investment programme. This device is Trust property and must be used in accordance with this policy and our Acceptable Use Policy. All Trust laptops are encrypted and centrally managed via Microsoft Intune.

Software installation - You must not install any software, application, or browser extension on your trust device unless it is available through the Company Store. This applies even to free or well-known tools. If you need a specific application for your work, submit a request via the helpdesk and the Digital team will review and, if appropriate, add it to the store.

Updates and patches - Your device is managed centrally via Microsoft Intune. Security updates will be applied automatically. You must not defer or disable update prompts. Our software and devices are kept up to date with the latest updates from software developers, hardware suppliers and vendors, to prevent attackers from leveraging known vulnerabilities - including vulnerabilities exploited via phishing-delivered malware.

Physical security - You must not leave your laptop unattended, including within school premises. You must never leave your laptop in your car. When stepping away from your desk, you must lock your screen immediately.

7. Access Control and Identity

The Trust operates on the principle of least privilege: staff are given access only to the systems and data they need to carry out their role. Access rights are reviewed periodically and removed promptly when a member of staff changes role or leaves the Trust. Privileged accounts - those with access to sensitive information, financial assets, or IT administration - are limited to the absolute minimum needed, and are regularly reviewed to ensure continued need. Accounts that are no longer being used are removed or suspended.

7.1 Your Account

Your trust account gives you access to systems and data appropriate to your role. You are responsible for all activity carried out under your credentials. You must:

- Never share your password with anyone, including IT staff - we will never ask for your password
- Use a strong, unique password for your trust account
- Lock your screen or log out when leaving your device unattended
- Not use your trust email address to register for personal or non-work services

7.2 Multi-Factor Authentication (MFA)

MFA is required to access trust systems, and is used wherever practical so that an attacker cannot access an account using a stolen password alone. You will need to verify your identity using a second factor - typically the Microsoft Authenticator app - in addition to your password. MFA significantly reduces the risk of your account being compromised even if your password is obtained by someone else.

You must not approve MFA prompts that you did not initiate. If you receive an unexpected approval request, you must decline it and contact the helpdesk immediately.

7.3 Geographic Access Restrictions

Trust systems are configured to block login attempts from high-risk countries. This protects against unauthorised access from territories identified as elevated risk. If you are travelling abroad and need to access trust systems, you must notify the Digital team in advance so that appropriate access can be arranged.

Attempting to circumvent geographic access controls - for example by using a VPN or proxy to mask your location - is a serious breach of this policy.

7.4 Privileged and Administrative Access

A small number of staff hold administrative or elevated access rights. These accounts carry greater risk and are subject to additional controls:

- Privileged accounts must only be used for tasks that require elevated access
- Day-to-day work such as email and browsing must use a standard account
- All use of privileged accounts is logged and subject to periodic review

8. Phishing and Social Engineering

Our school environment makes staff a credible target for phishing, particularly for attacks impersonating HMRC, the DfE, exam boards, or senior leaders within the Trust. Staff should be aware that phishing attacks may increasingly use AI-generated content to appear more convincing, including realistic messages, impersonation, or automated responses.

8.1 What to Look For

Be alert to emails or messages that:

- Create urgency or pressure you to act quickly
- Ask you to click a link, open an attachment, or provide credentials
- Come from an address that looks slightly wrong (e.g. @invictus.educati0n rather than @invictus.education)
- Claim to be from a senior colleague asking for an unusual favour, especially involving payments, gift cards, or sensitive information
- Arrive unexpectedly, even if they appear to come from a known contact

8.2 What to Do

- If you are unsure about an email, you must not click any links or open any attachments. Contact the helpdesk for advice.
- If you have clicked a suspicious link or opened a suspicious attachment, you must report it to the helpdesk immediately. Do not wait to see if anything happens - speed is critical, and early reporting significantly limits the damage that can be done.
- If you receive an unexpected MFA approval request, you must decline it and report it to the helpdesk immediately.
- You must never provide your password, MFA code, or personal details in response to an email or phone call, regardless of who the sender claims to be.

8.3 Reporting is Encouraged

We operate a no-blame culture when it comes to reporting suspected phishing. If you report something promptly, you are helping to protect everyone, and giving the Trust vital information about the types of attack being targeted at our organisation - as well as situations where legitimate emails are being mistaken for phishing. Staff will not be penalised for reporting in good faith, even if the email turns out to be legitimate.

All staff will receive regular phishing awareness training. Staff in roles identified as higher risk - such as those with financial authority or access to sensitive data - will receive more frequent, targeted training. This includes succinct learning videos based on real examples and case studies, and online interactive learning activities such as quizzes and gamified exercises.

8.4 Simulated Phishing Campaigns

We run simulated phishing campaigns, supported by in-person reinforcement, to help staff build and maintain safe habits. The no-blame culture described above applies to the genuine reporting of suspected phishing; it is separate from the process below, which addresses staff who click links within these simulations:

- An initial click sees the staff member receive an 'on-the-spot' notification and a short learning video
- Upon a second click, the staff member will receive a detailed training video, plus a session with their line manager to ensure they fully understand the need for vigilance
- Further clicks will lead to formal disciplinary action

Where staff members demonstrate consistent unsafe behaviours, evidenced through simulated phishing responses, the Trust will enact formal disciplinary procedures, notwithstanding the support and encouragement provided at earlier stages.

8.5 Reducing Our Exposure

Attackers use publicly available information about our Trust and its staff to make phishing (and particularly spear-phishing) messages more convincing. This is often gleaned from our website and social media accounts - information sometimes referred to as our 'digital footprint'. All staff need to be conscious of the impact of:

- Information shared on our websites and social media pages - what do visitors need to know, and what detail is unnecessary but could be useful to an attacker?
- What our partners give away about our Trust online
- How sharing personal information has the potential to affect both them and the Trust

9. Cyber Incident Response

A cyber security incident is any event that could compromise the security of our systems, data, or devices. Examples include clicking a phishing link, ransomware, a lost or stolen device, an unexpected account lockout, or unusual activity on a system.

9.1 Your Immediate Responsibilities

You must report all suspected incidents to the helpdesk as soon as possible. You must not attempt to investigate or resolve the issue yourself, as this can inadvertently destroy evidence or make matters worse.

When reporting, include:

- What happened and when
- Which device or system was involved
- Any actions you already took

If instructed by the Digital team to disconnect your device from the network or power it off, you must do so immediately.

9.2 How Incidents are Classified and Managed

The Digital team will assess and classify all reported incidents:

Level	Description	Examples
Low	Isolated, contained, no data loss	Blocked phishing attempt, failed login from unknown location
Medium	Potential compromise, limited impact	Successful phishing click, lost device, suspected malware
Critical	Active attack or confirmed breach	Ransomware, confirmed data exfiltration, widespread system compromise

Critical incidents will trigger the Trust's Business Continuity Plan and the Digital Team's Disaster Recovery Plan. The CEO and Trust Single Point of Contact will be notified immediately of any critical incidents.

We recognise that all organisations will experience security incidents at some point, so it is crucial that we are able to detect them quickly and respond in a planned way to limit the harm caused. Technical security monitoring capability - described in Section 5 - helps us pick up on incidents that users may not become aware of themselves.

9.3 Legal Reporting Obligations

Where an incident involves the loss or unauthorised access of personal data, the Trust has a legal obligation under UK GDPR to notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. The Head of Digital Transformation and the Data Protection Officer are responsible for making this determination and filing the notification. Staff must therefore report suspected data breaches without any delay - the 72-hour clock starts from when the Trust first becomes aware, not when the incident occurred.

10. Contact Information

If you feel this policy has been violated, or you are unsure how it applies to a situation you have encountered, you have a number of resources available to help you, including your immediate line manager, your headteacher, the Central Services Helpdesk, and the policy lead listed above. We will follow the relevant Trust policies for any reported violation.

11. Compliance

All staff are expected to comply with this policy. Failure to do so may result in disciplinary action in line with the Trust's disciplinary procedures. Where a breach constitutes a criminal offence - for example, unauthorised access to systems or deliberate data destruction - it may be referred to the relevant authorities.

12. Glossary of Terms

Phishing: Fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details, for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Malware (malicious software): Any program or file that is harmful to a computer user, including computer viruses, worms, Trojan horses, and spyware.

Two-factor / Multi-factor authentication: A system whereby you are required to have two (or more) forms of identification to access your account, be it a password and an authenticator app, a password and an SMS message, etc.

DMARC, SPF, DKIM: Email authentication standards used to verify that a message genuinely originates from the domain it claims to, making it harder for attackers to spoof trusted email addresses.

Digital footprint: The trail of information about an organisation or individual that is publicly available online, for example via websites and social media, which attackers may use to make phishing attempts more convincing.

13. Parental Impact Assessment

As part of the policy review process, consideration has been given to whether the policy, or any changes to it, has a direct impact on parents and carers. This includes assessing whether changes affect parental responsibilities, required actions, communication processes, or understanding of Trust or school practices.

Decision:

The Trust Executive Team has determined that parental communication is:

- ❖ Not required for this policy