Cyber Security

Approved by:	Kristian Still	**Position:**	COO
Last reviewed:	January 2026	**Next review due:**	January 2028

*Electronic approval on file

Monitoring arrangements
This policy will be reviewed bi-annually and in line with our DPO recommendations.

Author: E Barnard	Title: CCTV	Ref: IE01-016	Date: January 2026
Inclusion Education is the working name of Inclusion Education CIO registered number 1162711			

Contents

Aims, Scope and Principles

Inclusion Education maintains Cyber Essentials certification to ensure a strong baseline of cyber security across the organisation. This includes applying the five core controls: secure configuration, boundary firewalls, user access control, malware protection, and regular patching. Cyber security has been identified as a risk for Inclusion Education, and every employee needs to contribute to ensure data security.

Inclusion Education has invested in technical cyber security measures but we also need our employees to be vigilant and to act to protect the organisations IT systems.

Our IT service provider supports Inclusion Educations responsibility for cyber security.

If you are an employee, you may be liable to disciplinary action if you breach this policy.

This policy supplements other data management and security policies, namely our Data Protection Policy, Data Breach Policy, Information Security Policy, Acceptable Use Policy, Home Working Policy, Electronic Information and Communications Policy.

1. What is Cyber-Crime?

Cyber-crime is simply a criminal activity carried out using computers or the internet including hacking, phishing, malware, viruses or ransom attacks.

The following are all potential consequences of cyber-crime which could affect an individual and/or individuals:

- Cost – The global cost of all forms of online crime is estimated to be in excess of £300 billion. We may be fined up to £17.5 million or 4% of the total worldwide annual turnover if we fail to protect our data.

- Confidentiality and data protection - Protecting individuals' confidential information and all forms of personal data is one of the most essential requirements for all Inclusion Education sites. Risk to confidential information and personal data is the biggest of all threats from cyber-crime.

- Potential for regulatory breach – We have various regulatory duties which we could unintentionally breach through falling victim to cyber-crime or a cyber-attack. Loss of personal data can lead to claims for damages by the individuals concerned and/or significant fines from the Information Commissioners Office (ICO).

- Reputational damage – A cyber security incident can have a major impact on our reputation, particularly if it involves the loss of confidential information, personal data and/or is reported in the media. Protecting our reputation is of utmost importance.

- Business interruption – Some forms of cyber-attack could render key systems (for instance servers including email servers, cloud computing services or our website) unavailable. This would have a major impact on delivering lessons and delivering our services. It may be necessary in such cases to invoke our Business Continuity Plan. The Head of Business Operations is responsible for making that decision and communicating with IT.

- Structural and financial instability – The financial losses flowing from online crime may cause or contribute to financial difficulty.

3. Cyber-Crime Prevention

Given the seriousness of the consequences noted above, it is important for Inclusion Education to take preventative measures and for staff to follow the guidance within this policy.
This cyber-crime policy sets out the systems we have in place to mitigate the risk of cyber-crime. The Head of Business Operations can provide further details of other aspects of the Inclusion Education risk assessment process upon request.

Inclusion Education has put in place a number of systems and controls to mitigate the risk of falling victim to cyber-crime. These include technology solutions as well as controls and guidance for staff.

3.1 Technology Solutions

Inclusion Education has implemented the following technical measures to protect against cyber-crime:

- firewalls;
- anti-virus software;
- anti-spam software;
- auto or real-time updates on our systems and applications;
- URL filtering;
- encryption;
- deleting or disabling unused/unnecessary user accounts;
- deleting or disabling unused/unnecessary software;
- using strong passwords; and

- disabling auto-run features.

3.2 Controls and Guidance for Staff

- All staff must follow the policies related to cyber-crime and cyber security as listed in this policy.
- Technology solutions in isolation cannot protect us adequately, so our systems and controls extend to cover the human element of cyber-crime/cyber security risk.
- All staff will be provided with training at induction and refresher training as appropriate; when there is a change to the law, regulation or policy; where significant new threats are identified and in the event of an incident affecting the Inclusion Education or any third parties with whom we share data.
- It may be appropriate in some instances to limit the number of people involved or who have access to information on a matter to ensure the security of the data involved. This can be part achieved through IT security measures. We may implement other controls that are more practical in nature.
- Physically ringfencing the individuals or teams working on a matter;
- Taking steps to ensure our system for opening, distributing and/or scanning incoming correspondence (by post, email or otherwise) does not allow or inadvertent sharing of confidential information;
- Disposing of confidential documents securely;
- Having a clear desk policy;
- Discouraging staff from reading confidential papers or discussing sensitive matters in public.

Due diligence – we may conduct due diligence on the cyber security controls and cyber-crime prevention measures that other parties with whom we share information.

All staff must:

Ensure you are familiar with the risks presented by cyber-crime and cyber security attacks or failures and take appropriate action to mitigate the risks by taking a sensible approach, e.g. not forwarding chain letters or inappropriate/spam emails to others. We will help you by continually raising awareness of those risks and providing training where necessary.
Report any concerns you may have.

4. Passwords

- Choose strong passwords (Inclusion Educations IT team advises that a strong password contains; at least 8 characters, including both numbers, letters upper case and lower case , be changed on a regular basis, not be obvious or easily guessed (e.g., birthdays or other memorable dates, memorable names, events, or places etc.).
- keep passwords secret;
- Passwords should be changed immediately if you suspect your account has been compromised
- You must not write down your password(s) electronically in clear text (unencrypted).
- never reuse a password;
- Where available, multi-factor authentication (MFA) should be enabled on your account and for most systems this will be mandatory;
- never allow any other person to access the organisations systems using your login details;
- not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on their computer, phone or network or Inclusion Educations IT systems;
- report any security breach, suspicious activity or mistake made that may cause a cyber security breach, to the Head of Business Operations as soon as practicable from the time of the discovery or occurrence. If your concern relates to a data protection breach you must follow our Data Breach Policy;
- only access work systems using computers or phones that Inclusion Education owns. Staff may only connect personal devices to the guest Wi-Fi provided;
- not install software onto your work computer or phone. All software requests should be made to Senior Leadership team in the first ins; and
- avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using Inclusion Education equipment and/or networks.

Inclusion Education considers the following actions to be a misuse of its IT systems or resources:

- any malicious or illegal action carried out against Inclusion Education or using the organisations systems;
- accessing inappropriate, adult or illegal content within the premises or using the organisations equipment;
- excessive personal use of the IT systems during working hours;
- removing data or equipment from Inclusion Education premises or systems without permission, or in circumstances prohibited by this policy;
- using Inclusion Education equipment in a way prohibited by this policy;
- circumventing technical cyber security measures implemented by Inclusion Educations IT team;

and

- failing to report a mistake or cyber security breach.

5. Cyber-Crime Incident Management Plan

The incident management plan consists of four main stages and is overseen by our IT Service Provider.

1. *Containment and recovery:* To include investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost. We will notify our insurers as soon as reasonably practicable of any circumstances that may give rise to claim under relevant insurance policies. We will also assess whether it is necessary to invoke our business continuity plan.
2. *Assessment of the ongoing risk:* To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed and any consequences of the breach/attack identified.
3. *Notification:* To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
4. *Evaluation and response:* To evaluate future threats to data security and to consider any improvements that can be made.

Where it is apparent that a cyber security incident involves a personal data breach, Inclusion Education will invoke their Data Breach Policy rather than follow out the process above.

Inclusion Education IT Service provider is Greenpoint Computer Services:
Email: servicedesk@gpoint.co.uk
Phone: 01252 544788