

THE HUB EDUCATIONAL SERVICES CIC

Cyber Attack Policy

Date of Issue: October 2025 Review Date: October 2026 Approved by: Vanessa Brooks and Ellie Lupton

Purpose

The Hub Educational Services CIC recognises the critical importance of protecting its digital systems, data and infrastructure from cyber attacks. This policy establishes the organisation's approach to preventing, detecting, responding to and recovering from cyber incidents. Its purpose is to safeguard learner, staff and organisational data, maintain continuity of education and ensure full compliance with legal, regulatory and safeguarding requirements. The policy sets out clear expectations for all users of The Hub's digital systems and provides a structured framework for managing cyber risks effectively.

Scope

This policy applies to every individual who interacts with The Hub's digital environment, including staff, learners, governors, trustees, contractors, external professionals, visitors and third-party service providers. It covers all digital devices, networks, cloud systems, online services, software platforms and data storage solutions connected to or used by the organisation. Any person accessing or using The Hub's IT systems is required to comply with this policy at all times.

Definition of a Cyber Attack

A cyber attack is defined as any unauthorised attempt to access, damage, alter, corrupt or disrupt The Hub's digital systems, data or services. This includes, but is not limited to, malware infections, ransomware attacks, phishing attempts, denial-of-service attacks, insider threats, social engineering, account compromise, unauthorised access, data loss, misconfiguration exploitation and any other malicious digital activity that threatens the confidentiality, integrity or availability of organisational data and systems.

Responsibilities

The Senior Leadership Team and Digital Lead are responsible for ensuring that this policy is implemented, regularly reviewed and clearly communicated to all relevant parties. They oversee cyber risk assessments, business continuity planning and the strategic development of cyber resilience across the organisation.

The Data Protection Officer and Information Governance Lead monitor the implications of cyber incidents, assess whether personal data breaches have occurred and liaise with regulatory bodies such as the Information Commissioner's Office when required.

The IT Manager or external IT provider manages technical controls, system monitoring, backups, incident detection and technical response. They ensure that systems remain secure, updated and resilient.

All staff and learners must follow the Acceptable Use Policy, remain vigilant to cyber risks and report any security concerns or suspected incidents immediately.

The governing body and trustees provide strategic oversight of cyber resilience and ensure that adequate resources, training and infrastructure are in place to protect the organisation.

Prevention and Controls

The Hub adopts a proactive approach to cyber security. Cyber risk assessments are conducted at least annually and reviewed termly to ensure emerging threats are identified and mitigated. All software, firmware and hardware are kept up to date, and unsupported systems are disabled or replaced to prevent vulnerabilities. Strong authentication methods, including multi-factor authentication, are used wherever possible, and robust password policies are enforced.

Access to systems and data is restricted on a need-to-know basis to reduce exposure to risk. Regular data backups are performed and stored securely, and restoration processes are tested to ensure reliability. Staff, learners and governors receive ongoing cyber security awareness training, including guidance on phishing, social engineering, password safety and device protection.

An Acceptable Use Policy governs the behaviour of staff, learners and visitors when using digital systems. Third-party providers are required to meet appropriate cyber security standards, and internet access is filtered and monitored to reduce exposure to malicious content.

Incident Response and Reporting

Detection and Initial Response

If a cyber attack is suspected, such as unusual network activity, encrypted files or the appearance of a ransom demand, the IT Manager must be alerted immediately. Systems believed to be compromised should be isolated to prevent the spread of the

attack. Staff and learners must stop using affected systems and disconnect devices if instructed.

Containment and Investigation

The IT team will investigate the incident and document what occurred, including the time, method, affected systems, data involved and whether personal data may have been compromised. The Senior Leadership Team and Data Protection Officer will assess risks to learners, staff and safeguarding. Business continuity and learning continuity plans will be activated to ensure education delivery continues despite disruption.

External Reporting

If a personal data breach has occurred or is suspected, the organisation will notify the Information Commissioner's Office within 72 hours where required by UK GDPR. Significant cyber incidents will be reported to the Department for Education's sector team or other relevant education incident-reporting mechanisms. The organisation may also report incidents to the National Cyber Security Centre or Action Fraud, depending on the nature and severity of the attack.

Recovery and Post-Incident Review

Systems will be restored from backups once it is safe to do so. Credentials will be changed, logs reviewed and system integrity tested. A full lessons-learned review will be conducted, and the risk register, policy and technical controls will be updated accordingly. The incident and its outcomes will be reported to governors and trustees.

Business Continuity and Learning Continuity

The Hub maintains a Business Continuity Plan and Learning Continuity Plan that specifically address major cyber incidents. These plans ensure that alternative delivery methods, including paper-based and offline resources, are available to maintain learning during digital outages. Clear communication procedures are in place to inform parents, carers, staff and learners in the event of an extended system outage.

Training and Awareness

All staff and learners receive cyber security awareness training during induction and annually thereafter. This training covers phishing, social engineering, password security, device safety and general cyber hygiene. Regular refreshers, posters and updates reinforce safe digital practices. Specialised training is provided to high-risk users such as administrators, senior leaders and staff with access to sensitive data.

Monitoring, Audit and Assurance

The Hub maintains a detailed incident log for all cyber or security incidents. Regular audits of user accounts, access rights and network logs are conducted to ensure

ongoing security. Governors and trustees are informed at least termly about the organisation’s cyber-security status, including incidents, risks and mitigation measures. The organisation may seek external certification, such as Cyber Essentials, to demonstrate compliance and strengthen assurance.

Policy Review

This policy will be reviewed annually or sooner if a significant cyber incident occurs, if technology changes or if legislation is updated.