Vista
EDUCATION

Cyber Security Policy

A cybersecurity incident can have a major impact on any organisation for extended periods of time. For a training provider, this can range from minor reputational damage and the cost of restoring systems from existing backups, to major incidents such as losing student work or significant data breaches.

This Cybersecurity Policy outlines Vista Education's guidelines and security provisions which are there to protect our systems, services and data in the event of a cyberattack.

Physical Security

Vista Education does not have any significant IT infrastructure. Our IT is largely limited to laptops and computers. However we will ensure there is appropriate physical security and environmental controls to protect access to items of IT

User Accounts

Users are responsible for the security of their own accounts. If at any time they believe their credentials may have been compromised in such a way as to affect Vista Education or its learners, they must change their password and inform all relevant parties as soon as possible.

Vista Education accepts that personal accounts might be used for work purposes. However Vista Education requires all those involved in the delivery of courses and qualifications to implement robust security measures such as multi-factor authentication.

Devices

To ensure the security of all Vista Education expects that:

- Screen locks are used when devices are left unattended
- Security updates are implemented when prompted – including suitable anti-virus software
- Lost or stolen equipment is reported as soon as possible where there could be any implication for Vista Education or its learners
- If possible accounts are locked and passwords are changed for all accounts when a device is lost or stolen

Devices will be configured with the following security controls as a minimum:

Data Security

Vista Education will take appropriate measures to reduce the likelihood of the loss of confidential data such as:

- Personally identifiable information as defined by the ICO
- Special Category personal data as defined by the ICO
- Unpublished financial information

Data will be backed up wherever possible using a 3-2-1 backup methodology

- 3 versions of data e.g. own laptop, external drive, cloud
- 2 different types of media – Local HD and Cloud for critical material
- 1 copy of critical data offsite (e.g. hard drive in another location securely stored or a cloud backup)

Sharing Files

Vista Education recognises the security risks associated with sending and receiving confidential data. To minimise the chances of a data breach colleagues are required to:

- Consider if an email could be a credential phishing/scam email or that a colleague's account could have been 'hacked'. If something does not feel right, check with the sender by another method, particularly in relation to financial transactions, attachments, or links to websites
- Verify the recipient of data prior to sending
- Using file encryption where possible, sending passwords/keys via alternative communication channels
- Be Wary of attachments and links in emails: Avoid clicking on links or downloading attachments from unknown or unexpected emails.

- Pro-actively plan for the replacement of network hardware, operating systems and software before vendors stop providing security support for them
- Actively manage anti-virus systems
- Actively manage and test backups
- Regularly review and update security controls that are available with existing systems
- Segregate wireless networks used for visitors' & staff personal devices from school systems
- Review the security risk of new systems or projects

Incident Response Plan

Vista Education will develop and review a Disaster Recovery plan. This plan will be proportionate and based on the size of the organisation

- Categories and severities of a “disaster”
- Risk assessments
- Processes to follow in order to attempt data recovery
- Roles and responsibilities
- Who to contact (ICO, learners, Awarding organisations etc)

Policy Review: this policy will be reviewed annually as a minimum.

Responsible Person: Sue Ward

Created: November 2024

Date of next review: August 2025