HAMBLIN EDUCATION TRUST

Cyber Security Policy

Objective

The purpose and objective of this Cyber Security Policy is to protect the digital assets[1] of the Hamblin Education Trust[2] from all potential threats, whether internal or external, deliberate or accidental, to ensure normal school operations and business continuity and to minimise reputational damage.

Policy

- The Chief Financial Operations Officer has approved the Cyber Security Policy.
- It is the Policy of the Hamblin Education Trust to ensure that:
    1. Information will be protected from loss of confidentiality[3], integrity[4] and availability[5].
    2. Regulatory and legislative requirements will be met[6].
    3. IT services will be maintained and tested[7].
    4. Cyber security training will be available to all staff.
    5. All information security and data breaches, actual or suspected, will be reported to, and investigated by, the Head of IT Operations, and that Employees have clear instruction on what to do if such an incident occurs.
    6. Training is given to all employees to ensure safe and correct use of IT facilities and the data held by any member of the Trust.
    7. Data accessed remotely (for example by employees working at home) is done so in a secure manner.
    8. Security is maintained with Trust IT equipment used at home by employees and that such equipment is used appropriately.
    9. A policy on how to engage with social media[8] is in effect and communicated to, and understood by, all employees.
    10. Job applicants are screened and checked before employment.
- Guidance and procedures will be produced to support this policy. These may/will include incident handling, information backup, system access, virus controls, passwords and encryption.
- The role and responsibility of the Chief Financial Operations Officer is to ensure all employees are sufficiently aware of their responsibilities under the Cyber Security Policy and to ensure that all employees receive sufficient training and guidance.

- The role and the responsibility of the Head of IT Operations is to manage information security and to provide advice and guidance on implementation of the Cyber Security Policy.
- The Chief Financial Operations Officer and Head of IT Operations have direct responsibility for maintaining and reviewing the Cyber Security Policy. The Policy will be reviewed annually.
- All employees are directly responsible for implementing the Cyber Security Policy within their areas.
- It is the responsibility of each employee to adhere to the Cyber Security Policy.

Notes

1. Information takes many forms and includes data held digitally, printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, or spoken in conversation.
2. The Hamblin Education Trust refers to the Trust itself and its member schools.
3. Confidentiality: ensuring that information is only accessible to authorised individuals.
4. Integrity: safeguarding the accuracy and completeness of information and processing methods.
5. Availability: ensuring that authorised users have access to relevant information when required.
6. This includes the requirements of legislations such as the Companies Act, the Data Protection Act, the General Data Protection Regulation, the Computer Misuse Act and the Copyright, Designs and Patents Act.
7. The responsibility of the Head of IT Operations is to ensure that information and vital services are available to users whenever they need them.
8. Social media refers to any publicly available media communications platform such as Facebook, Twitter, Instagram, Snapchat, Whatsapp and others.