IT Code of Conduct Policy for Employees

Objective

The purpose and objective of this IT Code of Conduct Policy is to ensure safe and proper use of the computer systems[1] of the Hamblin Education Trust[2].

Policy

- The Chief Financial Operations Officer has approved this IT Code of Conduct Policy.
- It is the Policy of the Hamblin Education Trust to ensure that:
  1. Suitable IT facilities are provided for employee Trust use.
  2. Internet access is provided for employees to share data and information, to communicate with employees, parents, pupils and organisations/persons of a school related nature, and to conduct research.
  3. Email is provided for school related communications.
  4. Data or information stored on the system, or any message (via email or otherwise), should, in most instances, remain private. The Trust reserves the right to view any content stored or posted via the system as part of any authorised investigation into non-compliance.
  5. The use of removable media (for example memory sticks) is banned due to the ease of which viruses can be spread from them.

- Employees of the Trust are expected to:
  1. Use the computer system for authorised activities in conjunction with the requirements of their job function. Any use of the facilities for non-school related work may fall foul of the Computer Misuse Act (1998).
  2. Be responsible for their use of the system. General employee rules and guidelines apply.
  3. Store on the system content relevant to their employment only.
  4. Not violate regulatory and legislative requirements[3].
  5. Report any damage to computer systems to the Trust IT Technical Support Team through the Spiceworks ticketing system.
- The Chief Financial Operations Officer and the Head of IT Operations will review the Policy annually.

Non-compliance

The Trust may take action against any employee who deliberately:

- And maliciously causes the failure of any computer system.

- And maliciously causes the loss of data.
- And maliciously causes a data breach. Sharing of private data relating to pupils and employees with unauthorised persons or organisations may be in breach of the Data Protection Act and the General Data Protection Regulation. If in doubt, employees should seek permission before sharing such data.
- Uses the computer system to view unsuitable material, unless instructed to as part of an authorised investigation.
- Uses the computer system to engage in unsuitable communications[4]. This includes the use of the internet or wireless network to send such communications.
- Violates copyright through use of the system.

Action will be taken internally or in conjunction with the Police.

Data breaches and potential threats

- If, when using the computer systems, a data breach occurs, whether accidental or deliberate, employees must immediately inform the Chief Operations Officer and Head of IT Operations Manager of the nature and scope the breach.
- Employees must immediately inform the Head of IT Operations if they receive a suspicious or inappropriate email or other such communication.

Use of IT suites

IT suites are provided for teaching and training:

- Booking of a suite is via the IT Room Booking facility.
- Pupils should not be left unattended in IT suites. Employees may be held responsible for any damage done in a suite during a period in which they have booked the suite or when they are timetabled in it.

Use of social media and email for communication with pupils

- The Trust reminds employees of the need for caution when using Trust provided email and social media[5] for communication. Where possible, employees are reminded to stick to using Trust provide digital communication methods.
- The Trust cannot support any employee who engages in unsuitable communications with pupils.

Leaving employment

- Employees are expected to return any provided IT equipment before their final day of employment.
- User accounts for support staff will be disabled 1 day after the final day of employment.
- User accounts for teaching staff will be disabled at their contract expiry date.
- Employees are expected to transfer to another employee/shared workspace any documents/email they hold that are needed by the Trust before their final day of employment.

Access to other employee accounts

- Access to other employees' accounts cannot be given.
- If a document/email is required from a disabled account, a request must be made to the Chief Financial Operations Officer (for support and finance content) or the Head of IT Operations (for other content). The corresponding content will then be forwarded on to you.

Notes:

1. The Trust's computer systems encompass IT networks, cloud-based facilities including Office 365, school/Trust assigned email, use of social media and management information systems (SIMS and PS Financials), reprographic equipment and any personally supplied IT equipment.
2. The Hamblin Education Trust refers to the Trust itself and its member schools.
3. 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.
4. Unsuitable communications include any content on or via the system, or on social media which brings the School into disrepute, constitutes as bullying, or deemed as sharing inappropriate messages with pupils or other employees.
5. Social media refers to any publicly available media communications platform such as Facebook, Twitter, Instagram, Snapchat, Whatsapp and others.