IT Code of Conduct Policy for Visitors

Objective

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

Policy

• It is the Policy of the Hamblin Education Trust to ensure that:

1. 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.

2. The use of removable media (for example memory sticks) is banned due to the ease of which viruses can be spread from them.

• Visitors of the Trust are expected to:

1. Limited personal use of Trust IT systems (internet, email) is allowed as long as it does not interfere with job responsibilities or violate Trust policies. Excessive personal use, or use for personal gain, is prohibited and may result in disciplinary action.

2. Be responsible for their use of the system. General visitor rules and guidelines apply.

3. Adhere to the Trust's data retention policies and ensure that sensitive data is securely deleted when no longer required. The improper disposal of data, including sending sensitive data to personal email accounts or using

unapproved services, is prohibited.

6. Not violate regulatory and legislative requirements.

7. Report any damage to computer systems to the Trust IT Technical Support Team through the Spiceworks ticketing system.

Non-compliance

The Trust may take action against any visitor 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 visitors with unauthorised persons or organisations may be in breach of the Data Protection Act and the General Data Protection Regulation. If in doubt, visitors should seek permission before sharing such data.
- Uses the provided internet access to view unsuitable material, unless instructed to as part of an authorised investigation.
- Uses the provided access to engage in unsuitable communications. 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.

Accountability for devices

- Visitors are responsible for the proper care and security of their personal devices when connected to the network.