Horizons Specialist Academy Trust

Staff Electronic Device Policy

Adopted by Finance and General Purposes committee: 22 May 2018
Date of Next Review: May 2020
Responsible Officer: ICT Manager

Statement of intent

Horizons Specialist Academy Trust accepts that both trust-owned and personal electronic devices are widely used by members of staff. The Trust has a sensible and practical approach which acknowledges the use of devices and with this in mind, this policy is intended to ensure that:

- Members of staff are responsible users, and remain safe while using the internet.
- Trust ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.
- A process is in place for claiming financial payments when electronic devices are lost or damaged by members of staff.

Electronic devices can enhance work and learning opportunities, and enable people to be creative. In return, members of staff need to agree to be responsible users.

1. Legal framework

1.1. This policy has due regard to statutory legislation including, but not limited to, the following:

- The Computer Misuse Act 1990
- The Communications Act 2003
- The General Data Protection Regulations (2016)
- The Freedom of Information Act 2000
- The Human Rights Act 1998

1.2. This policy will be implemented in conjunction with the following Trust policies:

- GDPR Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- ICT Policy
- E-security Policy
- Disciplinary Policy and Procedure
- Photography and Video Policy
- Acceptable usage agreement

2. Roles and responsibilities

2.1. The board of directors has overall responsibility for ensuring that this policy, as written, does not discriminate on any grounds, including, but not limited to, the following:

- Ethnicity
- National origin
- Culture
- Religion
- Gender
- Disability
- Sexual orientation

2.2. The CEO is responsible for handling complaints regarding this policy as outlined in the Trust's Complaints Policy.

2.3. The ICT Manager is responsible for the day-to-day implementation and management of the policy.

2.4. The ICT Manager is responsible for ensuring that all Trust-owned electronic devices have security software installed, in order to protect sensitive data in cases of loss or theft.

3. Acceptable use

3.1. The Trust monitors the use of all ICT systems and electronic devices.

3.2. Members of staff only use Trust-owned electronic devices for educational purposes.

3.3. Usernames and passwords are not disclosed to others.

3.4. Programmes and software are not installed on Trust-owned electronic devices without permission from the ICT Manager.

3.5. Staff are not permitted to remove any software from a Trust-owned electronic device without permission from the ICT Manager.

3.6. Members of staff who install or remove software from a Trust-owned electronic device without seeking authorisation from the ICT Manager, may be subject to disciplinary measures.

3.7. Trust-owned electronic devices are not used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

3.8. Any illegal, inappropriate or harmful activity is immediately reported to the ICT Manager.

3.9. All antivirus software is updated at least every month.

3.10. Members of staff do not open email attachments from unknown sources.

3.11. Members of staff do not use programmes or software which may allow them to bypass the filtering or security systems.

3.12. All data is kept confidential, in accordance with the Trust's GDPR Data Protection Policy.

3.13. Members of staff only use Trust-owned electronic devices to take pictures or videos of people who have given permission.

3.14. Trust-owned electronic devices are not used to access social media websites unless permission has been given by the ICT manager for work purposes.

3.15. Trust-owned electronic devices are not used to communicate with pupils or parents/carers unless on official Trust business.

3.16. Members of staff ensure that they have permission to access learning materials from unapproved sources.

3.17. Copyrighted material is not downloaded or distributed.

3.18. Trust equipment that is used outside the premises, e.g. laptops, will be returned to the Trust when the employee leaves employment, or if requested to do so by the ICT Manager.

3.19. Failure to adhere to the rules described in this policy may result in disciplinary action.

4. Loaning electronic devices

4.1. Trust equipment, including electronic devices, may be loaned to staff.

4.2. The ICT Team is responsible for the maintenance and day-to-day management of the equipment, as well as the loans process.

4.3. By loaning Trust equipment and electronic devices, staff members are agreeing to act in accordance with the terms of acceptable use.

4.4. Once a request has been authorised, the staff member will be required to undergo any training required to use the requested equipment, including how to store, handle and undertake any maintenance, e.g. changing batteries.

4.5. If the equipment or device is no longer required, staff members will inform the ICT Manager of this as soon as possible, allowing the equipment to be made available to someone else.

5. Portable equipment

5.1. All data is synchronised with the Trust server at least once a month.

5.2. Members of staff ensure that all Trust-owned electronic devices are made available for anti-virus updates and software installations, patches or upgrades, at least once a month.

5.3. Portable Trust-owned electronic devices are not left unattended, and are kept out of sight when they are not in use.

5.4. Portable equipment is transported in its protective case, if supplied.

5.5. Where the Trust provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, only these devices are used.

6. Personal devices (including phones)

6.1. Staff members will use personal devices in line with the Trust's E-Security Policy.

6.2. Members of staff do not contact pupils or parents/carers using their personal devices.

6.3. Personal devices are only used for off-site educational purposes when mutually agreed with the CEO.

6.4. The Trust is not responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

6.5. Inappropriate messages are not sent to any member of the Trust community.

6.6. Members of staff bringing personal devices into Trust ensure that there is not any inappropriate or illegal content on their device.

6.7. During lesson times, unless required for the teaching activity being undertaken, personal devices are kept in a lockable cupboard housed in the staffroom or classroom.

6.8. Under no circumstances should personal data be stored on a non Trust device.

7. Removable media

7.1. Removable media is not to be used for any purpose unless agreed by the ICT manager prior to its usage.

7.2. Where removable media is used it must be securely stored.

7.3. Personal and confidential information will not be stored on removable media.

7.4. Removable media is disposed of securely by the Trust ICT Team.

8. Cloud-based data storage

8.1. The Trust is aware that data held in remote and cloud-based storage is still required to be protected in line with the Data Protection Act 1998.

8.2. Members of staff ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

9. Liability for loss or damages

9.1. For the purpose of this policy, 'damage' is defined as any fault in a Trust-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT Manager

- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

9.2. The Trust's insurance covers Trust-owned electronic devices that are damaged or lost, during Trust hours, if they are being used on the Trust premises.

9.3. If a Trust-owned electronic device is damaged or lost outside of Trust hours or off-site, the member of staff at fault may be responsible for paying damages.

9.4. Staff members must use Trust-owned electronic devices within the parameters of the Trust's insurance cover, to ensure that the insurance policy is not void in the event of a claim – otherwise the staff member responsible may be required to pay for damage or loss.

9.5. Any incident which leads to a Trust-owned electronic device being lost is treated in the same way as damage.

9.6. The ICT Manager decides whether a device has been damaged due to the actions described above.

9.7. The Trust ICT Team is contacted if a Trust-owned electronic device has a technical fault.

9.8. If it is decided that a member of staff is liable for the damage, they may be required to pay for the cost of repair or replacement cost.

9.9. A written request for payment is submitted to the member of staff who is liable to pay for damages.

9.10. If the member of staff believes that the request is unfair, they can make an appeal to the CEO, who makes a final decision within two weeks.

9.11. In cases where the CEO decides that it is fair to seek payment for damages, the member of staff is required to make the payment within six weeks of receiving the request.

9.12. Payments are made to the Trust's Head of Finance & Operations, and a receipt is given to the member of staff.

9.13. The CEO may agree for the payment to be made in instalments.

9.14. In cases where a member of staff repeatedly damages Trust-owned electronic devices, the CEO may decide to permanently exclude the member of staff from accessing devices.