Brontë Academy Trust

Great schools. Inspirational people. Strong foundations.

Bronte Academy Trust Staff ICT and Electronic Devices Policy

Reviewed By	Approved By	Date of Approval	Version Approved	Next Review Date
Working Party	JB	8 Feb 19		8 Feb 21
GH	JB	13 Jan 20		13 Jan 22
DH	SC	27 Sep 22		27 Sep 24
DH / Trustees	Trust Board	28 Jan 25		28 Jan 27

Contents

STATEMENT OF INTENT

Bronte Academy Trust believes that ICT plays an important part in both teaching and learning over a range of subjects, and the Trust accepts that both trust-owned and personal electronic devices are widely used by members of staff. The Trust is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work.

The Trust has a sensible and practical approach that acknowledges the use of devices, and 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

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, and the Social Media Policy.

1. LEGAL FRAMEWORK

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)

This policy operates in conjunction with the following Trust Policies

- Data Protection Policy
- Freedom of Information Policy
- Complaints Procedures Policy
- Disciplinary Policy and Procedure
- Finance Policy
- Records Management Policy

2. ROLES AND RESPONSIBILITIES

The Trust board has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The headteacher is responsible for:

- The day-to-day implementation and management of the policy
- The overall allocation and provision of resources.
- Handling complaints regarding this policy as outlined in the Trust's Complaints Procedures Policy
- Informing staff that the Trust reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy

The ICT technician is responsible for:

- Carrying out checks on internet activity of all user accounts and to report any inappropriate use to the headteacher
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to the headteacher
- Ensuring routine security checks are carried out on all Trust-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed
- Ensuring that, thorough appropriate steps will be taken to ensure personal information is not seen during security checks, staff are made aware of the potential risks
- Accessing files and data to solve problems for a user, with their authorisation
- Adjusting access rights and security privileges in the interest of the protection of the Trust's data, information, network and computers

- Disabling user accounts for staff who do not follow this policy, at the request of the headteacher
- Assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy
- Assisting staff with authorised use of ICT facilities and devices, if required
- Immediately reporting any breach of trust owned devices to the DPO

Staff members are responsible for:

- Requesting permission from the headteacher or ICT technician, subject to their approval, before using Trust owned devices for personal reasons during school hours
- Requesting permission to loan Trust equipment and devices from the headteacher
- Requesting permission from the headteacher, subject to their approval, before using personal devices during school hours and ensuring these devices are submitted for security checks
- Ensuring any personal devices that are connected to the Trust are encrypted
- Reporting misuse of ICT facilities or devices, by staff or pupils to the headteacher
- Reading and signing a Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use Trust owned and personal devices

The Office Manager is responsible for:

- Ensuring value for money is secured when purchasing electronic devices
- Monitoring purchases made under the finance policy
- Overseeing purchase requests for electronic devices

3. CLASSIFICATIONS

Trust owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors, interactive displays and projectors
- Speakers, amplifiers, AV receivers and microphones
- Keyboards and mice
- Cameras
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Servers, network switches and wireless access points
- Photocopying, printing and reproduction equipment
- Documents and publications (any type of format)

4. ACCEPTABLE USE

This policy applies to any computer or other device connected to the school's network and computers.

The Trust will monitor the use of all ICT facilities and electronic devices. Members of staff will only use Trust owned and approved personal devices for work duties and educational purposes. The

duties for which is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews etc
- Researching any Trust-related task
- Any Trust encouraged tuition or educational use
- Collating or processing information for Trust business
- Communicating with other members of staff, such as contacting the school office for assistance

Inappropriate use of Trust owned and personal devices could result in a breach of the Trust's Data Protection Policy.

Inappropriate use of Trust owned and personal devices could result in a breach of legislation including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the Trust's Data Protection Policy or relevant legislation will face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

.

Since ICT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the ICT facilities will be reported to the headteacher.

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

Any illegal, inappropriate or harmful activity will be immediately reported to the headteacher.

Members of staff will not:

- Open email attachments from unknown sources
- Use programmes or software that may allow them to bypass the filtering or security systems
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels

Members of staff will only use Trust owned electronic devices to take pictures or videos of people who have given their consent.

Trust-owned electronic devices will not be used to access personal social media accounts.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the Trust online

- Avoid disclosure of any confidential information or comments regarding the Trust, or any information that may affect its reputability
- Have the necessary privacy settings applied to any social networking sites

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought

Copyrighted material will not be downloaded or distributed.

Trust owned devices will be taken home for work purposes only, once approval has been sought from the headteacher.

Trust equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested by the headteacher.

While there is scope for staff to utilise Trust equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Personal use of Trust-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of Trust facilities for personal reasons. A charge may be made for using equipment if the values are significant.

Where permission has been given to use the Trust equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to the headteacher.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. EMAILS AND THE INTERNET

The Trust email system and internet connection are available for communication and use on matters directly concerned with Trust business.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proof read by the staff member sending the email to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

The Trust will be liable for any defamatory information circulated either within the school or to

external contacts.

The school email system and accounts will never be registered or subscribed to spam or other non work-related updates, advertisements or other personal communications. Trust email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

Personal email accounts will only be accessed via school computers outside of work hours. Staff will ensure that access to personal emails never interferes with work duties.

Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the Trust to any obligations by email or the internet without ensuring that they have the authority to do so.

Purchases for Trust equipment will only be permitted to be made online with the permission of the CFO, and a receipt will be obtained in order to comply with monitoring and accountability. Hard copies of the purchase will be made for the purchaser and the CFO. This is in addition to any purchasing arrangement followed according to the Trust's Finance Policy.

6. PORTABLE EQUIPMENT

All data on Trust-owned equipment will be synchronised with the school server and backed up at least once per month.

Portable Trust-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked when they are not in use.

Portable equipment will be transported in its protective case, if supplied.

7. PORTABLE DEVICES

Staff members will use personal devices in line with the school's Data and E-Security Breach Prevention and Management Policy.

Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner.

Members of staff will not contact pupils or parents using their personal devices.

Personal devices will only be used for off-site educational purposes when mutually agreed with the headteacher.

Inappropriate messages will not be sent to any member of the school community.

Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

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

8. REMOVABLE MEDIA

Only recommended removable media will be used including, but not limited to, the following:

- USB Portable Storage Drives
- Optical Discs

All removable media will be securely stored in a safe location when not in use.

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

Staff, with support the ICT technician will encrypt all removable media with appropriate security measures where applicable.

Removable media will be disposed of securely by the ICT technician.

9. CLOUD-BASED STORAGE

Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

10. STORING MESSAGES

Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

If a member of staff is unsure about the correct message storage procedure, help will be sought from the ICT technician.

Employees who feel that they have cause for complaint as a result of any communications on Trust owned devices will raise the matter initially with the headteacher, as appropriate. The complaint will then be raised through the grievance procedure in line with the Grievance Policy.

11. UNAUTHORISED USE

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit authorisation from the headteacher
- Physically damage ICT and communication facilities or Trust owned devices
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the ICT technician or headteacher. Certain items are asset registered, their location is recorded by the Office Manager for accountability. Once items are moved after authorisation, staff will be responsible for notifying the Office Manager of the new location.
- Use or attempt to use someone else's user account.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal

- Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisation
- Online gambling
- Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
- Any sexually explicit content, or adult or chat-line phone numbers

- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else
- Install hardware or software without the consent of the ICT technician
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the Trust computers
- Use or attempt to use the Trust's ICT facilities to undertake any form of piracy, including the infringement of software licences or other copyright provisions whether knowingly or not. This is illegal
- Purchase any ICT facilities without the consent of the ICT technician or headteacher. This is in addition to any purchasing arrangements followed according to the Finance Policy
- Use of any chat lines, bulletin boards or pay to view sites on the internet. In addition, staff will not download or attempt to download any software of this nature
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher. This is in addition to any purchasing arrangement followed according to the Finance Policy
- Knowingly distribute or introduce a virus or harmful code onto the Trust's network or computers. Doing so may result in disciplinary action, including summary dismissal
- Use the ICT facilities for personal use with the authorisation of the headteacher. This authorisation will be requested on each occasion of personal use
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material
- Use or attempt to use, the communication facilities to call overseas without the authorisation of the headteacher
- Obtain and post on the internet, or send via email, any confidential information about other employees, the Trust, its customers or suppliers
- Interfere with someone else's use of the ICT facilities
- Be wasteful of ICT resources, particularly printer ink, toner and paper
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victims genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of Trust owned devices, they will report this immediately.

12. PURCHASING

Individual staff members will not be permitted to purchase equipment or devices, or process payments for such goods, on the Trust's behalf unless permission has been sought from the headteacher.

The cost of any equipment or devices personally purchased by staff members will not be reimbursed by the Trust unless otherwise specified by the headteacher.

The Office Managers will seek advice from the ICT technician and professionals when purchasing equipment.

All equipment and electronic devices will be sourced from a reputable supplier.

The ICT technician will maintain an Asset Register which will be used to record and monitor the Trust's ICT assets. All equipment and electronic devices purchased using Trust funds will be added to this register.

When devices are not fit for purpose, or are at least **four** years old, staff members may request new equipment. If their request is granted, the old equipment or electronic device will be returned to the Office Manager, including any accessories which were originally included with the device. Any old devices will then be disposed of or securely erased by the ICT technician.

13. SAFETY AND SECURITY

The Trust's network will be secured using firewalls in line with the Data and Cyber-security Breach Prevention and Management Policy.

Filtering of websites, as detailed in the Data and Cyber-security Breach Prevention and Management Policy, will ensure that access to websites with known malware are immediately reported to the ICT technician and blocked.

Approved anti-virus software and malware protection will be used on all applicable devices and will be configured to update on a regular basis.

Staff will report suspicious emails to the ICT technician whom will also utilise administrative tools to detect and block spam, malware and phishing transmitted via email.

Members of staff will ensure that all Trust-owned electronic devices are made available for audits, anti-virus updates, malware protection updates and software installations, patches or upgrades when requested by the Headteacher or ICT technician.

Programmes and software will not be installed on school-owned electronic devices without permission from the ICT technician.

Staff will not be permitted to remove any software from a Trust owned electronic device without permission from the ICT technician.

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

All devices will be secured by a password or biometric access control.
Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Further security arrangements are outlined in the Data and Cyber-security Breach Prevention and Management Policy

14. LOSS, THEFT AND DAMAGE

For the purpose of this policy, **"damage"** is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

The Trust's insurance will cover Trust owned electronic devices that are damaged or lost.

Staff members will use Trust-owned electronic devices within the parameters of the Trust's insurance cover.

Any incident that leads to a Trust-owned electronic device being lost will be treated in the same way as damage.

The ICT technician and headteacher will decide whether a device has been damaged due to the actions described above.

The ICT technician will be contacted if a Trust-owned electronic device has a technical fault.
If it is decided that a member of staff is liable for the damage, they will be required to pay 20 percent of the total repair or replacement cost. A written request for payment will be submitted to the member of staff who is liable to pay for damages.

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

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

Payments will be made to the Office Manager via the main office, and a receipt is given to the member of staff.

The Trust will accept payments made via cheques and cash.

A record of the payment will be made and stored in the main office for future reference.

The headteacher may accept the payment in instalments.

If the payment has not been made after six weeks, the fee will increase by five percent and continues for a maximum of six months – at which point formal disciplinary procedures will begin.

The member of staff will not be permitted to access Trust-owned electronic devices until the payment has been made.

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

If a Trust-owned device is lost or stolen, or is suspected of having been lost or stolen, the DPO will be informed as soon as possible to ensure the appropriate steps are taken to delete data from the device that relates to the Trust, its staff and its pupils, and that the loss is reported to the relevant agencies.

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

15. IMPLEMENTATION

Staff will report any breach of this policy to the headteacher.

Use of the telephone system will be logged and monitored.

Use of the Trust internet connection will be recorded and monitored.

The ICT technician may remotely view or interact with any of the computers on the Trust's network. This may be used randomly to implement this policy and to assist in any difficulties.

The Trust's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.

The Trust's database systems are computerised. Unless given permission by the ICT technician, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.

Attempting to access the database using another employee's user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.

User accounts will be accessible by the headteacher and the ICT technician.

Users will ensure that critical information is not stored solely within the Trust's computer system.

Hard copies will be kept or stored separately on the system. If necessary, documents will be password protected.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

16. MONITORING AND REVIEW

This policy will be reviewed bi-annually by the ICT technician and Trustees

Any changes or amendments to this policy will be communicated to all members of staff.

Declaration of Responsibility

This Staff ICT and Electronic Devices Policy was reviewed and formally adopted by Bronte Academy Trust on

.....28 Jan 25.....Date

....Signed Chair of Trustees

.....Signed Chief Executive Officer