KEYSTONE
ACADEMY TRUST

IT and Devices Acceptable Use Policy

Updated by Tracey Roscher October 2023	Ratified by Trustees October 2023
Next Review due October 2024	

Contents

1. Device and technology acceptable use agreement for staff

Whilst our Trust promotes the use of technology or devices and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the **headteacher** for any necessary further action to be taken.

The Trust reserves the right to monitor its communication systems and services. This includes, but is not limited to, email, telephone conversations, electronic messaging, internet use, and system access. Monitoring is used by the Trust for the following purposes:

- To maintain and ensure security of systems and information;
- To check for unauthorised use;
- To establish facts relevant to school business;
- To ensure quality assurance and ensure that procedures are being followed;
- To undertake disciplinary, performance, and capability proceedings; and
- To prevent or detect crime.

The Trust uses Securely web filtering to report on web searches and websites that are being accessed by staff and pupils to ensure compliance with Keeping Children Safe In Education 2023.

All Trust laptops make use of Bitlocker encryption and two-factor authentication applies when logging into the network outside of schools or the Trust.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors. The Trust IT network and equipment are subject to access controls to ensure only authorised persons can access.

Please read this agreement carefully, and sign at the bottom to show you agree to the terms outlined.

2. Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the school's **Data Protection Policy** and any other relevant school policies and procedures.
- Operate a clear screen policy when I leave my device unattended e.g. locking my computer screen.

- Protect portable devices and removable media at all times. When not in use they will be subject to appropriate security e.g. placed out of sight or under lock and key.
- Ensure all portable IT equipment used to store or process sensitive information, such as personal data, is encrypted.
- Ensure all IT equipment is returned to Headteacher/Executive Headteacher when no longer required. This is to ensure devices are securely wiped or destroyed.
- Only access or attempt to access IT systems that I have been authorised to access.
- Only access or attempt to access information for official school purposes aligned with my role and this must be on a need-to-know basis.

I will not:

- Attempt to bypass any filtering, monitoring and security systems.
- Share school-related password with pupils, staff, parents or others.
- Use the username and password of another person or share my own username and password with another person.
- Misuse, bypass or change the configuration or security settings of any IT system or equipment.
- Introduce unauthorised software, hardware, or removable media.

3. Using technology in school

I will:

- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time. Personal use of the Internet must be reasonable, proportionate, and occasional.
- Only use recommended removable media and keep this securely stored.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the headteacher or ICT technician.
- Search for, view, download, upload or transmit any inappropriate material when using the internet.
- Process or access racist, sexist, defamatory, offensive, obscene, illegal or otherwise inappropriate material.
- Carry out illegal, fraudulent or malicious activity.
- Use school or Trust IT systems or equipment to carry out or support business which is unrelated to the school.
- Break copyright or carryout any activity that negatively impacts intellectual property rights.

4. Emails

I will:

- Only use the approved email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.
- Check that the recipients of e-mail are correct before sending to avoid accidental release to unintended recipients. I will take particular care when using auto complete in my email client, as an unintended email address may be used in error. If a data breach occurs by sending information to the incorrect recipient, I will report immediately to the Headteacher/Executive Headteacher, who will discuss with the DPO.
- Take care when opening an attachment or clicking on any link within any email unless confident the email is legitimate.
- Delete suspicious emails and forward to our IT technician Sean.Casey@turniton.co.uk for further investigation/blocking.
- Use the blind carbon copy (BCC) feature when sending an email to more than one recipient and it is necessary to protect email addresses.
- Use password protected documents when sending sensitive information via email.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

5. School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the headteacher.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices only as directed by the ICT technician.
- Seek permission from the headteacher before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.

- Immediately report any damage or loss of my school-owned devices to the headteacher.
- Immediately report any security issues, such as downloading a virus, to the ICT technician.
- Understand that I am expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.
- Make arrangements to return school-owned devices to the headteacher upon the end of my employment at the school.

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the headteacher.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

6. Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices to communicate with pupils or parents.
- Access the school's WiFi using a personal device unless permission to do so has been granted by the headteacher or ICT technician.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any school-related information on personal devices unless permission to do so has been given by the headteacher.

7. Removable Media

I will:

- Ensure removable media which contains sensitive information such as personal data is encrypted. Removable media includes USB flash drives, CDR, DVDR, removable hard drives.

I will not:

- Introduce removable media from an unknown source to the school IT network as it may contain malware designed to harm school systems.

8. Social media and online professionalism

I will:

- Follow the Trust Staff Code of Conduct regarding use of social media.
- Understand that I am representing the school and Trust and behave appropriately when posting on school or Trust social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept ‘friend’ or ‘follow’ requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the school on any social media platforms or other online platforms which may affect the school’s reputation.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

9. Working from home

I will:

- Ensure no unauthorised persons, such as family members or friends, access any devices used for home working.
- Ensure that reasonable safeguards are taken to manage the increased likelihood of a security incident.
- Only remove IT equipment from school premises when there is a clear business need and when authorised to do so.

- Prevent inadvertent disclosure of information and avoid being overlooked when working.
- Avoid storing IT equipment in an unoccupied vehicle unless more secure options are unavailable. Unless unavoidable, I will place the equipment out of sight, in the locked boot of the vehicle.
- Connect portable devices to the Trust network on at least a monthly basis in order to receive security updates. I will ensure devices remain connected until such time updates have been received and applied i.e. Windows updates.

I will not:

- Store IT equipment in a vehicle overnight.

10. Training

I will:

- Participate in any relevant training offered to me, including annual NCSC cyber-security training and online safety.
- Allow the ICT technician and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- Deliver any training to pupils as required.

11. Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- Understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- Understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

12. Reporting Security Incidents

I will:

- Report all security incidents and suspected security incidents in accordance with the school's Cyber Response and Recovery Plan.

- Stop what I am doing, power off the IT equipment and report it immediately if I identify suspicious activity while using IT equipment or believe I am the victim of malware e.g. a virus.
- Report all security incidents to Sean.Casey@turniton.co.uk and the headteacher immediately.

13. Review

This policy shall be reviewed annually.

---

14. Agreement

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Name	
Signature	
Date	