Policy name:	Acceptable Use Policy
Author(s):	Lyssy Bolton
Date written:	May 2023
Date ratified:	
Date amended:	
Next review date:	May 2024

Contents

Aims 2
Role of the Headteacher and Senior Leadership Team 2
Linked Policies 3
Acceptable Use Agreement 3
School personnel will: 4
School personnel will not: 4
Signature: 5
Appendix 1 6

Aims

- Ensure school personnel are aware of all legislation relating to computer misuse, data protection and copyright
- Share good practice within the school
- Protect children from the risk of radicalisation and extremism
- Ensure compliance with all relevant legislation connected to this policy
- Work with other schools and the local authority to share good practice in order to improve this policy
- Systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- To make users aware that internet use by school personnel is monitored by the Trust for safeguarding purposes

Role of the Headteacher and Senior Leadership Team

The Headteacher and the Senior Leadership Team will:

- Ensure all school personnel are aware of and comply with this policy
- Ensure all school personnel sign and date the 'Acceptable Use of ICT Agreement'
- Provide guidance, support and training to all staff
- Make effective use of relevant research and information to improve this policy
- Monitor the effectiveness of this policy
- Lead the development of this policy throughout the school
- Display these guidelines around the school
- Provide guidance and support to all staff
- Keep a log of all ICT equipment available to school personnel and a register of equipment issued to staff and volunteers
- Provide training for all staff on induction and when the need arises
- Undertake risk assessments when required

Linked Policies

- Safeguarding and Child Protection

Acceptable Use Agreement

The Mead Trust recognises the important contribution and value that technology can play in promoting children's learning and development. However, there are potential risks involved. We have rigorous procedures and practices in place and have taken positive steps to reduce risk in each school as we believe that the benefits to children from accessing the internet, in the form of information resources, and opportunities for collaboration, exceed any disadvantages. Allowing the use of mobile devices is a school decision, and should be subject to the following key principles:

- All individuals are protected from inappropriate material, bullying and harassment
- Users have access to resources to support learning and teaching
- Users should be given clear boundaries on responsible and professional use
- The school internet facility must be used only for educational purposes

Access to network services is given to users who act in a considerate, appropriate and responsible manner. Users are responsible for their behaviour on school networks just as they are in any part of each school. Access is a privilege, not a right, and entails responsibility. We expect all users to use technology (both that belonging to each school or their own), responsibly and strictly, according to the following conditions (for the purposes of this document, technology means any device that provides a connection to the internet or internal network):

- School property: A device loaned to a user by a school for an education related purpose, remains the property of The Mead Trust
- Connection to the school network: Only approved user devices may connect to a school network by prior agreement
- Device usage: A device must remain in the user's possession, should only be used by the user, and should be securely stored when not in use
- Data protection policies: The Mead Trust policies, regarding the appropriate use and sharing of information, apply to both school- and privately-owned devices. Use of any device must adhere to data protection, online safety and Health & Safety rules
- Education purposes: Devices may be used for education-related purposes at the discretion, and under the supervision of, a teacher or responsible adult
- Personal information / data: If used to create or store personal information, including images and videos of pupils, users must fully comply with high standards of data protection as set out in the Data Protection Act 2018
- Passcodes: A device connecting to a school network may be configured with certain restrictions in place. Any settings that are passcode protected must not be changed
- Insurance cover provides protection for school-owned devices from the standard risks whilst the device is on site or in a user's home but excludes theft from a car or other establishment. Should the device be left unattended and be stolen, the user will be responsible for its replacement. Privately-owned devices remain the responsibility of the owner and will not be covered under a school insurance policy
- Checks: All devices, whether owned by a school or privately owned, may be subject to checks for compliance with Trust policies. Failure to comply or evidence of unacceptable use will result in sanctions or disciplinary action

Users have a personal responsibility to abide by the set rules and regulations when using the internet and should be aware of the consequences if they are breached. This may include:

- Withdrawal of user access
- Further monitoring of how the internet is used
- Disciplinary action
- Criminal prosecution

Users must report immediately to the DSL / DDSL any accidental access to inappropriate material or websites that they may have.

Users will:

- Set passwords in accordance with the NCSC's strong password guidance (https://www.ncsc.gov.uk/cyberaware/home#section_2)
- Immediately report any illegal, inappropriate or harmful material or incident they become aware of, to the DSL / DDSL
- Communicate with others in a professional manner
- Ensure that when they take and / or publish images of others they will do so with permission
- Only use social networking sites in school in accordance with the Trust's policies
- Only communicate with children and parents / carers using official Trust systems
- If their role requires me to use CPOMS Single Sign On, they will use a personal device for this purpose
- Check personal devices only in allocated breaks and when not in the presence of children
- Use a personal device to adhere to security protocols and confirm their identity when accessing school systems outside of a school site
- Follow the rules set out in this agreement when using personal devices to carry out school working tasks (for example accessing school email on non-school owned devices)
- Use the network and cloud-based systems as directed to ensure that data and documents are backed up and stored securely
- Always log on and fully log off devices to ensure that routine updates are carried out automatically. This includes the updates of Sophos to protect the devices and the integrity of the network
- Password protect any data that enables a third party to be identified when sending it outside of the local secure network
- Keep data private and confidential, unless it is essential to disclose such information for an appropriate purpose
- Ensure that all permission has been given to use the original work of others

School personnel will not:

- Access, copy, remove or otherwise alter any other user's files, without their express permission
- Use the internet in such a way that it will bring the school into disrepute
- Use inappropriate or illegal websites
- Download inappropriate material or unapproved software
- Use inappropriate language
- Produce, send out, exhibit or publish material that will cause offence to anyone
- Divulge their login credentials or passwords to anyone
- Use the login credentials or passwords of any other user
- Use a computer that is logged on by another user
- Use any social networking site inappropriately
- Use school email for private use
- Use personal email addresses for school or Trust business

- Use personal equipment to record images / video
- Open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if they have any concerns about the validity of the email
- Try to upload, download or access any materials which are:
    - Illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act)
    - Inappropriate
    - May cause harm or distress to others
- Try to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials
- Try (unless they have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work
- Install or attempt to install programmes of any type on a machine, or store programmes on a computer without permission
- Send any data that enables a third party to be identified within the local secure network; sensitive information of this kind should be saved to an appropriate location and the recipient notified of that location

Signature:

- I understand that this policy applies to my work and use of school internet technology in school, and off the premises, including my use of personal internet technology
- I understand that if I fail to comply with this policy, I could be subject to disciplinary action or Police involvement
- I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines
- As an employee or associated person of The Mead Trust, I agree that I shall treat all records, data and information, relating to the Trust, (including all verbal, written and electronic information), as strictly confidential, and will not convey any information beyond my remit within The Mead Trust

To sign this policy, please go to Microsoft Forms.

Appendix 1

We believe this policy should be a working document that is fit for purpose, represents the school ethos, enables consistency and quality across the school and is related to the following legislation:

- Computer Misuse Act 1990
- Misuse of Information Act 1990
- Health and Safety (Display Screen Equipment) Regulations 1992
- Data Protection Act 2018
- Human Rights Act 1998
- Freedom of Information Act 2000
- Equality Act 2010
- Counter Terrorism and Security Act 2015

The following documentation is also related to this policy:

- Data Protection and Security: A Summary for Schools (Becta 2004)
- The Safe Use of New Technologies (Ofsted)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children
- Equality Act 2010: Advice for Schools (DfE)
- Race Disparity Audit - Summary Findings from the Ethnicity Facts and Figures Website (Cabinet Office)
- Guidance for Safer Working Practices (February 2022)

We are aware that the Brexit transition period ended on 31 December 2020 and, therefore, UK organisations that process personal data must now comply with the:
DPA (Data Protection Act) 2018 and UK GDPR (General Data Protection Regulation) if they process only domestic personal data;
DPA 2018 and UK GDPR, and the EU GDPR if they process domestic personal data and offer goods and services to, or monitor the behaviour of, EU residents.
We believe information and communications technology includes all forms of computing, the internet, telecommunications, digital media and mobile phones. School personnel have clear responsibilities with regard to the use of all ICT equipment and ICT facilities. We require staff and volunteers to be responsible users and stay safe whilst using the internet and communication technologies.

This agreement applies to use of technologies (e.g. laptops, iPads, email, Seesaw, Google etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.

Any member of the school personnel that uses illegal software or access inappropriate websites when in school faces dismissal. All school personnel will be made aware of all legislation relating to computer misuse, data protection and copyright.

We expect all school personnel to sign and date the 'Acceptable Use of ICT Agreement' and be fully aware of and implement the internet safety policy. All school personnel have the duty to report any misuse of the ICT equipment or the ICT facilities of this school.

We have a duty to ensure the internet safety of all pupils within this school.

We have a duty to safeguard children, young people and families from violent extremism. We are aware that there are extremist groups within our country who wish to radicalise vulnerable children and to involve them in terrorism or in activity in support of terrorism. Periodic risk assessments are undertaken to assess the risk of pupils being drawn into terrorism. School personnel must be aware of the increased risk of online radicalisation, and alert to changes in pupil's behaviour. Any concerns will be reported to the Designated Safeguarding Lead.

We are aware that under the 'Counter-Terrorism and Security Act 2015' we have the duty to have 'due regard to the need to prevent people from being drawn into terrorism'. This duty is known as the Prevent duty and we believe it is essential that school personnel are able to identify those who may be vulnerable to radicalisation or being influenced by extremist views, and then to know what to do when they are identified.

We provide a safe environment where we promote pupils' welfare. Within this environment we work hard to build pupils' resilience to radicalisation and extremism by promoting fundamental British values and for everyone to understand the risks associated with terrorism. We want pupils to develop their knowledge and skills in order to challenge extremist views.

We as a school community have a commitment to promote equality. Therefore, an equality impact assessment has been undertaken and we believe this policy is in line with the Equality Act 2010.

We all have a responsibility to ensure equality permeates into all aspects of school life and that everyone is treated equally irrespective of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. We want everyone connected with this school to feel safe, secure, valued and of equal worth.

This policy applies to the governance community, Graduate Teachers, volunteers, and all members of our school communities who are authorised to use technology to further the objectives of the Trust and its schools. This includes all individuals who have been issued with school equipment and / or a school email address. It also applies to visitors and volunteers who may on occasions have access to the school internet and network, even if they do not have a school device or equipment.