2019 -2021

Potential in Everyone Academy Trust
CEO – David Whitehead

Acceptable Use Policy

Committee	Finance and Staffing
Version	1.0
Author	Linda Lucas
Approved on	12 July 2019
Signature	
New Review date	July 2021

Associated Documentation	

Contents

1. Policy Statement

The aim of this policy to intended to provide a framework for the use of Potential in Everyone Academy Trust's IT resources. It should be interpreted such that it has the widest application and so as to include new and developing technologies and uses, which may not be explicitly referred to.

It stipulates the constraints and practices that a user must agree to as a condition of access to the Trust's network or the internet. It also includes the use of Trust email and telephony equipment.

This policy applies to all information, in whatever form, relating to the Trust's business activities, and to all information handled by the Trust relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by the Trust or on its behalf.

2. Scope of the policy

This Policy applies to all users of the Potential in Everyone Academy Trust's facilities – staff, parents/carers, visitors, volunteers, contractors and pupils.

3. Adoption Arrangements and Date

This policy procedure was adopted by the Board of Directors of Potential in Everyone Academy Trust on 12 July 2019 and supersedes any previous policy.

4. Review of Policy

This policy will be reviewed by the Board of Directors every two years or earlier if there is a need.

5. Responsibilities of the Trust

The Trust is responsible for ensuring individuals are given clear direction on the extent and limits of their authority about IT systems and data.

6. Computer Access Control – Individual's Responsibility

Access to the Trust's IT systems is controlled using User IDs and passwords. All User IDs and passwords uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Trust's IT systems.
Individual's must **not**:

- Allow anyone else to use their user ID and password on the Trust's IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access Trust IT systems.
- Leave their password unprotected (for example writing it down).
- Perform any unauthorised changes to the Trust's IT systems or information.
- Attempt to access data that they are not authorised to use or access.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-PIEAT authorised device to the network or IT systems (unless a Non-Executive Director).
- Store Trust data on any non-authorised IT equipment (this includes unencrypted USB devices). Non-Executive Directors may store Trust data on encrypted devices
- Give or transfer Trust data or software to any person or organisation outside the Trust without the prior written authorisation of the Trust
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) unless a legal exception applies or unless the download is permitted by law (eg a DfE licence). .
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect Trust devices to the internet using non-standard connections.

7. Internet and Email Conditions of Use

Use of the Trust's internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to the Trust's property, interests or reputation in any way, not in breach of any term and condition of employment and does not place the individual or the Trust's in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet and email systems.

Individuals must **not**:

- Use the internet or email for the purposes of harassment or abuse.
- Use profanity, obscenities, or derogatory, defamatory or unlawful remarks in communications.
- Access, download, send or receive any data (including images), which the Trust considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to the Trust, alter any information about it, or express any opinion about the Trust's, unless they are specifically authorised to do this.
- Send personal data externally other than in accordance with data protection legislation.
- Forward the Trust's mail to personal email accounts (for example a personal Hotmail account), unless specifically authorised to do
- Make official commitments through the internet or email on behalf of the Trust unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property
- Download any software from the internet without prior approval of the IT Department.
- Connect the Trust's devices to the internet using non-standard connections.

8. Clear Desk and Clear Screen Policy

In order to reduce the risk of unauthorised access or loss of information, the Trust enforces a clear desk and screen policy as follows:

- Personal or confidential business information must be protected using security features provided for example secure print on printers.
- Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
- Care must be taken to not leave confidential material on printers or photocopiers.
- All business-related printed matter must be disposed of using confidential waste bins or shredders.

9. Working Off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Working away from the office must be in line with the Trust's lone working policy.
- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.
- Work may not be taken offsite that may be considered a breach of GDPR

10. Mobile Storage Devices

Mobile devices such as unencrypted memory sticks and removable hard drives must not be used at any time for confidential, personal or sensitive information. Only the Trust's authorised mobile storage devices with encryption enabled must be used, when transferring confidential, personal or sensitive data.

11. Software

Individuals must use only software that is authorised by the Trust on Trust computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on the Trust's computers must be approved and installed by the Trust's IT department.

Individuals must **not**:

- Store personal files such as music, video, photographs or games on the Trust's IT equipment.

12. Viruses

The IT department has implemented centralised, automated virus detection and virus software updates within the Trust's. All PCs have antivirus software installed to detect and remove any virus automatically.
Individuals must **not**:

- Remove or disable anti-virus software.
- Attempt to remove virus-infected files or clean up an infection, other than using approved the Trust's anti-virus software and procedures.

13. Telephony Equipment Conditions of Use

Use of the Trust's telephony equipment is intended for business use. Individuals must not use the Trust's telephony facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communication.

Individuals must **not**:

- Use the Trust's telephony equipment for conducting personal business
- Make hoax or threatening calls to internal or external destinations.
- Accept reverse charge calls from domestic or International operators without the prior written approval of the CEO or the Headteacher.

14. Actions upon Termination of Contract or Employment

All the Trust's equipment and data, for example laptops and mobile devices including telephones, smartphones, external memory devices and CDs/DVDs, must be returned to the Trust forthwith at the end of the contract or employment period.

All the Trust's data or intellectual property developed or gained during the period of employment remains the property of the Trust and must not be retained beyond termination or reused for any other purpose.

15. Monitoring and Filtering

All data that is created and stored on the Trust's computers is the property of the Trust.

Our systems enable us to monitor telephone, email, voicemail, internet and other communications. In order to carry out its legal obligations as an employer (such as ensuring employee compliance with the Trust's IT related policies), and for other business reasons, we may monitor use of systems including the telephone and computer systems, and any personal use of them, by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes, such as child safeguarding and the prevention and detection of fraud. The Trust will avoid opening personal emails unless it has a good reason to do so, such as a reasonable suspicion that an offence or breach of the employment contract or of the Trust's policies has been committed.

16. IT Security Breaches

It is an individual's responsibility to report suspected breaches of security policy without delay to a Trust senior leader.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action will follow in line with the Trust's disciplinary procedures.

17. References to Other Sources of Information

Computer Misuse Act 1990
Data Protection Act (2018) and General Data Protection Regulation

Appendix A: Acceptable Use Policy for Parents/Carers

Acceptable Use Policy for Parent/Carers

<<Insert Name of School>>

- I have read and discussed the Acceptable Use Policy for Children (attached) with my child.
- I know that my child will receive online safety (e-Safety) education to help them understand the importance of safe use of technology and the internet, both in and out of school.
- I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons and to safeguard both my child and the school's systems. This monitoring will take place in accordance with data protection and human rights legislation.
- I understand that the school will take all reasonable precautions to ensure that pupils cannot access inappropriate materials, but I appreciate that this is a difficult task. I understand that the school cannot be held responsible for the content of materials accessed through the Internet and the school is not liable for any damages arising from use of the Internet facilities.
- I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
- I understand that if my child does not abide by the school Acceptable Use Policy for Children then sanctions will be applied in line with the school's behaviour and anti-bullying policy. If the school believes that my child has committed a criminal offence, then the Police will be contacted
- I, together with my child, will support the school's approach to online safety (e-Safety) and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community
- I know that I can speak to the school Online Safety (e-Safety) Coordinator, my child's teacher or the Head Teacher if I have any concerns about online safety (e-Safety).
- I will visit the school website <***Insert School Website Address***> for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
- I will visit www.thinkuknow.co.uk/parents, www.nspcc.org.uk/onlinesafety, www.internetmatters.org www.saferinternet.org.uk and www.childnet.com for more information about keeping my child(ren) safe online.
- I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

I have read the Parent Acceptable Use Policy.

Child's Name…… Class……..……

Parent's Name…… Parent's Signature……..

Date……

Appendix B: Acceptable Use Policy for Staff

Acceptable Use Policy for Staff

<<Insert Name of School>>

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy

1. This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

2. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

3. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

5. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly. .

6. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

7. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 2018 and the General Data Protection Regulation 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls that meet the EU and UK regulations) or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. Any images or videos of pupils will only be used as stated in the school image use policy and will always consider parental consent.

8. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. Where possible I will use the school learning platform KLZ to upload any work documents and files in a password protected environment or via VPN. I will protect the devices in my care from unapproved access or theft.

9. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

10. I will respect copyright and intellectual property rights.

11. I have read and understood the school Online Safety (e-Safety) Policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

12. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead and/or the Online Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites Designated Safeguarding Lead and/or the Online Safety Coordinator and/or the designated lead for filtering as soon as possible.

13. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the ICT Technician as soon as possible.

14. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will always be transparent and open to scrutiny . All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Headteacher.

15. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

16. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, Potential in Everyone Academy Trust or the County Council, into disrepute.

17. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

18. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead and/or the Online Safety Coordinator or the Headteacher.

19. I will familiarise myself with the Online Safety Policy Appendices as they are published to staff.

20. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ……..... Print Name: ……. Date: ..…….

Accepted by: …….. Print Name: …….. Date: ……

Appendix C: Acceptable Use Policy for Visitors/Volunteers

Acceptable Use Policy for Visitors/Volunteers

<<Insert Name of School>>

1. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998 and the General Data Protection Regulation 2018. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school. If I am permitted access to any images or videos of pupils, I will only use them as stated in the school image use policy and will always consider parental consent

2. I have read and understood the school online safety (e-Safety) policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

3. I will follow the school's policy regarding confidentiality, data protection and the use of images and will abide with copyright and intellectual property rights, child protection legislation, privacy and data protection law, GDPR and other relevant civil and criminal legislation.

4. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will always be transparent and open to scrutiny . All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

5. My use of ICT and information systems will be compatible with my role within school. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. I will take appropriate steps to protect myself online and my use of ICT will not interfere with my work duties and will always be in accordance with the school AUP and the Law

6. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, the Potential in Everyone Academy Trust or the County Council, into disrepute.

7. I will promote online safety with the children in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

8. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead/ Head Teacher.

9. I will report any incidents of concern regarding children's online safety to the Designated Safeguarding Lead as soon as possible.

I have read and understood and agree to comply with the Visitor/Volunteer Acceptable Use Policy.

Signed: …….... Print Name: …… Date: ……..

Accepted by: …….. Print Name: …….. Date: ……

Appendix D: Wi-Fi Acceptable Use Policy

Wi-Fi Acceptable Use Policy

For those using school Wi-Fi

As a professional organisation with responsibility for children's safeguarding it is important that all members of the school community are fully aware of the school's boundaries and requirements when using the school Wi-Fi systems, and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. This is not an exhaustive list and all members of the school community are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.

Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The School takes no responsibility for the security, safety, theft, insurance and ownership of any device used within the School premises that is not the property of the School.

1. The use of ICT devices falls under Potential in Everyone Academy Trust's Acceptable Use Policy, online safety (e-Safety), policy and behaviour and child protection policies which all pupils, staff, visitors and volunteers must agree to and comply with.

2. The school reserves the right to limit the bandwidth of the wireless service, as necessary, to ensure network reliability and fair sharing of network resources for all users.

3. School owned information systems, including Wi-Fi, must be used lawfully and I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

4. I will take all practical steps necessary to make sure that any equipment connected to the school's service is adequately secure (such as up-to-date anti-virus software, systems updates).

5. The school's wireless service is not secure, and the school cannot guarantee the safety of traffic across it. Use of the school's wireless service is done at my own risk. By using this service, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network. For that reason, I expressly agree that I knowingly assume such risk, and further agree to hold the school harmless from any claim or loss arising out of, or related to, any such instance of hacking or other unauthorised use or access into my computer or device.

6. The school accepts no responsibility for any software downloaded and/or installed, e-mail opened, or sites accessed via the school's wireless service's connection to the Internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other Internet-borne programs is my sole responsibility; and I indemnify and hold harmless the school from any such damage.

7. The school accepts no responsibility regarding the ability of equipment, owned by myself, to connect to the school's wireless service.

8. I will respect system security and I will not disclose any password or security information that is given to me. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

9. I will not attempt to bypass any of the school security and filtering systems or download any unauthorised software or applications.

10. The school provides Wi-Fi for the school community and authorised visitors. My use of the school Wi-Fi will be safe and responsible and will always be in accordance with the school AUP and the Law including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

11. I will not upload, download, access or forward any material which is illegal or inappropriate or may cause harm, distress or offence to any other person, or anything which could bring the school into disrepute.

12. I will report any online safety (e-Safety) concerns, filtering breaches or receipt of inappropriate materials to the Designated Safeguarding Lead, the Online Safety (e-Safety) Coordinator and/or the designated lead for filtering as soon as possible.

13. If I have any queries or questions regarding safe behaviour online, then I will discuss them with the Online safety (e-Safety) Coordinator or the Headteacher.

14. I understand that my use of the school's internet will be monitored and recorded to ensure policy compliance in accordance with privacy and data protection and GDPR legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school will terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, then the matter will be brought to the attention of the relevant law enforcement organisation.

I have read and understood and agree to comply with the school's Wi-Fi Acceptable Use Policy.

Signed: ……..... Print Name: …… Date: ……

Accepted by: …….. Print Name: …….. Date: ……..