E-Safety Policy

Policy reviewed by Academy Transformation Trust on	September 2017

This policy links to:	Located:
• Safeguarding Policy • Data Protection Policy • Freedom of Information Policy • Disciplinary Procedure • Behaviour for Learning Policy • Social Media Policy	

Review Date – January 2020

Our Mission

To provide the very best education for all pupils and the highest level of support for our staff to ensure every child leaves our academies with everything they need to reach their full potential.

We promise to do everything we can to give children the very best education that gives them the best opportunity to succeed in life. All of our academies have it in them to be outstanding and achieving this comes down to our commitment to our pupils, staff and academies.

Our commitment

We are committed to taking positive action in the light of the Equality Act 2010 with regard to the needs of people with protected characteristics. These are age, disability, pregnancy and maternity, religion and belief, race, sex, sexual orientation, gender reassignment and marriage and civil partnership.

We will continue to make reasonable adjustments to avoid anyone with a protected characteristic being placed at a disadvantage.

We will measure the success of our commitment in this policy by analysing bullying logs and actions in our academies to reduce or eliminate incidents of bullying.

Introduction

Purpose and Ethos

Our academies use technology extensively across all areas of the curriculum. Online safeguarding (e-safety) is an area that is constantly evolving and as such this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner.

We have a duty of care to ensure that all our pupils, including those with SEN or a disability, are competent, informed, safe users of ICT and web-based resources. Understanding e-safety online is a life skill and empowering children from an early age to safeguard themselves and their personal information should be nurtured throughout their education to see them into adult life. We are committed to supporting teachers and parents to understand what safe internet use means, to identify and prevent potential risks and identify risky behaviour.

The purpose of this policy is:

- To empower the ATT community with the knowledge to stay safe and risk free
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeable harm to pupils or liability to The Trust.

This policy is available for anybody to read on the academy website.

At the start of each academic year, or on induction if part way through a year, staff and volunteers will participate in e-safety training in-line with safeguarding training and sign the Staff and Volunteers Acceptable Use Policy (Appendix 2). Upon signing the Acceptable Use Policy, staff and volunteers will be permitted access to academy technology including the internet. In signing the Staff and Volunteers Acceptable Use Policy or record sheet, staff and volunteers are also signing to confirm that they have read and understood the revised ATT E-Safety Policy.

All pupils and parents will sign a copy of the appropriate Pupil Acceptable Use Policy (Appendices 3 & 4) when they join the academy.

Parents/carers and pupils in EYFS, KS1 or KS2 will be required to sign a copy of the appropriate Pupil Acceptable Use Policy on progression to the next phase. Parents should be reminded of their agreement annually just as they should be, for example, with the photo consent agreement. On entry into a secondary academy, parents and pupils will be required to sign and return a copy of the appropriate Pupil Acceptable Use Policy.

Pupils in KS3, KS4 or KS5 are then required to revisit the Pupil Acceptable Use Policy annually and the academy is responsible for evidencing that this has occurred. Upon signing the appropriate Acceptable Use Policy, pupils will be permitted access to academy technology including the internet.

All pupils, including those with SEN or a disability, should be guided through the policy and the acceptable use of IT to ensure they understand risks and appropriate use and are able to make

the right choices when using IT and/or working online. This could also be discussed in parent/academy meetings on entry to ATT academies or at transition points.

Contents

1 Roles and Responsibilities

1.1 Academy Transformation Trust will:

1.1.1 Review this policy annually and in response to any e-safety incident to ensure that the policy is up to date. Appendix 1 should be completed as a record of key e-safety incidents to show where records are kept.

1.2 The Academy Committee will:

1.2.1 Ensure all aspects of technology within the academy meet the e-safety requirements within this policy.

1.2.2 Ensure e-safety incidents are properly dealt with and ensure policies and procedures are effective in managing those incidents.

1.2.3 The Governor with responsibility for safeguarding should include the governance of e-safety within their role and will:

- Keep up to date with emerging risks and threats including sexual exploitation, radicalisation and extremism through technology use.
- Receive regular updates from the Principal in regards to training, identified risks and incidents.
- Advise on changes to this policy.
- Monitor and ensure the effectiveness of e-safety training within the academy.
- Recommend further initiatives for e-safety training and awareness within the academy.

1.3 The Principal will:

1.3.1 Have overall responsibility for e-safety within their academy. The day-to-day management of this can be delegated to a Senior Leader with responsibility for e-safety. The Senior Leader with responsibility for e-safety (or Principal, if Senior Leader is not nominated) will be known as the E-Safety Officer for the purposes of this policy.

1.3.2 Delegate the responsibility for the technical elements of e-safety to a member of support staff. The member of staff with responsibility for the technical elements of e-safety will be known as ICT Support for the purposes of this policy.

1.3.3 Ensure e-safety training throughout the academy is planned and up to date and appropriate to the recipient (e.g. all staff, pupils, Senior Leadership Team (SLT), Academy Committee and parents).

1.3.4 Ensure that the E-Safety Officer has appropriate CPD to undertake their duties (e.g. CEOP training and WRAP). Annual and ongoing e-safety training is arranged for all staff, in line with safeguarding and as new guidance is shared.

1.3.5 Ensure that all e-safety incidents are dealt with appropriately and promptly in accordance with academy safeguarding procedures and that records are kept including details of the incident and action taken.

1.4 The E-Safety Officer/Lead will:

1.4.1 Keep up to date with the latest risks to children whilst using technology.

1.4.2 Review the policy regularly and bring any matters to the attention of the Principal.

1.4.3 Advise the Principal on e-safety matters.

1.4.4 Engage with parents and the academy community on e-safety matters within the academy and/or at home.

1.4.5 Liaise with ICT Support, the academy e-safety group (comprising of members identified by the academy to ensure e-safety best practice) and other agencies as required.

1.4.6 Keep a log of all e-safety incidents; ensure staff know what to report and ensure an appropriate audit trail.

1.4.7 Ensure technical e-safety measures within the academy are fit for purpose (e.g. internet filtering software; behaviour management software).

1.4.8 Ensure appropriate reporting procedures are in place (e.g. reporting function of internet filtering/monitoring software).

1.4.9 If the E-Safety Officer is not the Designated Safeguarding Lead (DSL) appropriate communication should be identified to ensure correct safeguarding procedures are in place.

1.5 The ICT Support will:

1.5.1 Be responsible for ensuring that the ICT technical infrastructure is secure and monitored; this will include ensuring the following:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Operating system updates are regularly monitored and devices updated as appropriate.
- Any e-safety technical solution such as internet filtering or monitoring are operating correctly.
- Filtering levels are applied appropriately and accordingly to the age of the user; that categories of use are discussed and agreed with the E-Safety Officer and Principal.
- Passwords are applied to **all** users regardless of age and are changed regularly. Passwords should be a minimum of eight characters for staff and secondary aged pupils.
- The Administrator password is changed regularly, with no reuse within 12 months with at least eight characters, upper and lower case letters; numbers and symbols.

1.6 Staff will ensure that:

1.6.1 They are aware that the use of equipment and software connected to the network is monitored.

1.6.2 They have completed e-safety training and signed the Acceptable Use Policy.

1.6.3 All details within the policy are understood and any uncertainty should be discussed with the E-Safety Officer and/or Principal.

1.6.4 Any e-safety incident is reported to the E-Safety Officer or the Principal in their absence and an incident report is made.

1.6.5 Promoting and sharing e-safety practices are planned for and embedded into curriculum practices.

1.7 All pupils will:

1.7.1 Understand the boundaries for the use of ICT equipment and services in the academy. These are given in the Pupil Acceptable Use Policy. Any deviation or misuse of ICT equipment and/or services will be dealt with in accordance to the Behaviour for Learning Policy.

1.7.2 Understand e-safety is embedded into the curriculum. Pupils will be given appropriate advice and guidance by staff. Pupils will be fully aware how they can report areas of concern or safety concerns including sexual exploitation and extremism within or outside the academy.

1.8 Parents and carers will:

1.8.1 Play the most important role in the development of their children and as such the academy will actively support parents and carers in obtaining the skills and knowledge they need to ensure the safety of children outside the academy environment. Through communication methods such as parents' evenings and academy newsletters, the academy will keep parents and carers up to date with new and emerging e-safety risks and will involve parents and carers in strategies to ensure children are empowered.

1.8.2 Understand the academy needs to have procedures in place to ensure that their children can be properly safeguarded. As such, parents and carers will receive a copy of the Pupil Acceptable Use Policy. Parents and carers should support the academy when sanctioning pupils for compromising the e-safety of themselves or others.

2 Technology

2.1 The academy uses a range of ICT devices. In order to safeguard the pupils and prevent loss of personal data, the following assistive technology is employed:

- **Internet Filtering**: software is used to prevent access to illegal websites. The academy has a Filtering Policy in place. It also prevents access to inappropriate websites. What is appropriate and inappropriate is determined by the age of the user and will be reviewed in line with this policy or in response to an incident, whichever is sooner. Filtering providers are members of the Internet Watch Foundation and systems block access to illegal Child Abuse Images and Content (CAIC). Filtering systems include the police assessed list of unlawful terrorist content, produced on behalf of the Home Office Systems. They are used to monitor and report online activity including email and website access in multiple languages. The E-Safety Officer and ICT Support are responsible for ensuring that filtering is appropriate and that any issues are brought to the attention of the Principal. The academy can determine the level of filtering at network level, to be age and group appropriate and to permit and deny content as required (this may be through third party support).
- **Network Monitoring**: monitoring software allows the tracking and reporting of incidents to safeguard users. If a device is used through the academy network it will be monitored both when connected and once reconnected after being used offsite. Monitoring occurs whilst using any aspect of the network and is not restricted to online use.
- **Reporting**: the academy provides the ability to report inappropriate content. Incidents are logged and shared with the DSL and/or SLT as appropriate. A log of website activity is kept.
- **Email Filtering**: every effort will be made to ensure emails are not infected including the use of software that prevents infected emails being sent from or received by the academy. Emails are monitored for inappropriate content.
- **Encryption**: all academy devices that hold personal data (as defined by the Data Protection Act 1998) are encrypted. No data is to leave the academy on an un-encrypted device. All devices that are kept on academy property and which may contain personal data are encrypted. Any breach (e.g. loss/theft of a device such as a laptop or USB key drives) is to be brought to the attention of the Principal who will act accordingly.
- **Passwords**: all staff and pupils will be unable to access any device without a unique username and password. Staff and pupil passwords will change on a regular basis. ICT Support will be responsible for ensuring that passwords are changed.
- **Anti-virus**: all capable devices will have anti-virus software. This software will be updated at least weekly for new virus definitions. ICT Support will be responsible for ensuring this task is carried out and will report to the Principal if there are any causes for concern. All USB peripherals such as key drives (if allowed) are to be scanned for viruses before use.

3 Safe Use

3.1 **Internet**: use of the internet in the academy is a privilege, not a right. Internet use will be granted to staff, volunteers and pupils upon completion of training and on signing the appropriate Acceptable Use Policy.

3.2 **Email**: all staff are reminded that emails are subject to Freedom of Information requests, this means emails should be of a professional, work-based nature and as such, written appropriately. Emails of a personal nature are not permitted. Pupils are permitted to use the email system and as such will be given their own email address.

3.3 **Photos and videos**: parents should sign a digital media (such as photos and videos) release slip on the pupils' entry to the academy, including Early Years. Non return of the permission slip will not be presumed as acceptance. You should also refer to the Social Media Policy for more information.

3.4 **Mobile phones and hand-held electronic devices**: pupils may only use mobile phones and wireless hand-held devices if specifically asked to by a member of staff and in line with the academy policy for the use of mobile phones (Appendix 5). Staff should ensure they follow academy policy on the use of mobile phones and in line with the following:

- Mobile phones should only be answered and in sight of administration areas of the building. Classroom based staff should store their mobile phones in a safe place away from the setting and should not access them in lesson and extra-curricular time. It is recommended that mobile phones are password protected and insured.
- Visitors, including contractors and parents/carers should be made aware of the **NO USE** policy on entry to the academy and through reminders such as posters and verbal reinforcement by members of staff accompanying them. Any photography required of the building (e.g. for estates purposes) should be completed when children are not present. Academy staff should challenge any use of mobile phones that does not adhere to this policy.

3.5 **Sexting**: in this case refers to 'youth produced sexual imagery' as defined by *Sexting in schools and colleges: Responding to incidents and safeguarding young people*, UKCCIS 2016. Imagery includes both moving and still images. We will ensure pupils are taught in an age appropriate manner the legal, social and moral issues around sexting. Pupils will be encouraged to report all incidents of sexting. Teaching staff will inform the DSL who will act according to the ATT Safeguarding Policy and the guidance outlined in the *Sexting in schools and colleges: Responding to incidents and safeguarding young people*, UKCCIS 2016.

3.6 **Radicalisation and Extremism**: the academy ensures pupils are safe from terrorist and extremist material when accessing the internet in school; this includes establishing appropriate levels of filtering. If a concern arises pupils will know who to go to and adults should inform the DSL who will act according to the ATT Safeguarding Policy and the guidance outlined in the Prevent and Channel Duty Guidance. The curriculum will ensure pupils are prepared positively for life in Modern Britain.

3.7 **Social Networking**: there are many social networking services available and the academy is fully supportive of social networking as a tool to engage and collaborate with learners and to engage parents and the wider academy community. You should refer to the ATT

Social Media Policy for a list of social media services permitted for use within the academy. These services have been appropriately risk assessed. Should staff wish to use other social media, permission must first be sought via the E-Safety Officer who will conduct a risk assessment. The Principal will then be able to determine whether permission should be granted based on the findings of the risk assessment and other relevant information.

In addition, the following restrictions must be adhered to:

- Permission slips must be consulted before images or videos of any child are uploaded
- Where services are set to 'comment enabled', comments must be set to 'moderated'
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the academy are not allowed unless the owner's permission has been granted or there is a license which allows for such use.

3.8 **Notice and Take-Down Policy**: should it come to the Trust's attention that there is a resource which has been inadvertently uploaded and is inappropriate, or the academy does not have copyright permission to use that resource, it will be removed within one working day.

3.9 **Incidents**: any e-safety incident is to be brought to the immediate attention of the E-Safety Officer or DSL depending on the processes and procedures in place, or in his/her absence, the Principal. The E-Safety Officer/DSL will assist you in taking the appropriate action to deal with the incident and fill out an incident log.

3.10 **Training and Curriculum**: it is important that the wider academy community is sufficiently empowered with the knowledge to stay as risk free as possible whilst using digital technology. This includes updated awareness of new and emerging issues including sexual exploitation and extremism. As such, the academy will provide information to parents and stakeholders regarding e-safety on request and promote e-safety where possible (e.g. e-safety display at parents evening). Consideration should be given to the delivery of key messages to pupils with SEN or a disability including specific examples for those issues directly relating to them.

3.11 E-safety for pupils is embedded into the curriculum and wherever ICT is used in the academy, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning.

3.12 As well as the programme of training the academy will establish further training or lessons as necessary in response to any incidents.

3.13 The E-Safety Officer is responsible for recommending a programme of training and awareness for the academy year to the Principal and the Safeguarding (e-safety) Link Governor for consideration and planning. Should any member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Principal for further CPD.

4 Trust and Academy websites

4.1 The ethos of ATT and the academy will be reflected in the website. Information will be accurate, appropriate, relevant, contemporary and well presented. Personal security and data will not be compromised. This will include the use of photographic material.

4.2 Permission will be obtained for the use of images on websites before any image or videos are used by ATT or academy websites.

4.3 The points of contact on ATT and academy websites will be the academy address, email and telephone number. There will be no information regarding staff or pupils' home data.

4.4 The Principal or nominated person will have overall editorial responsibility and ensure that this policy's expectations are met.

5 Education

5.1 Educating pupils about safety issues is essential in equipping them with the knowledge and skills to identify risks and take appropriate action. Key issues should be included within the IT/Computing curriculum, PSHE curriculum and where appropriate across the whole curriculum.

Appendix 1

E-Safety Officer/Designated Lead	**Name**: David Jenkins	**Contact Details**: david.jenkins@suttonacademy.attrust.org.uk
Technical Support Lead	**Name**: David Whitehead	**Contact Details**: David.whitehead@academytransformation.co.uk
Safeguarding (e-safety) Link Governor	**Name**: Paula Shrubsole	**Contact Details**: Paula.shrubsole@academytransformation.co.uk
E-safety group in place	**Members**: Dave Jenkins	**Contact Details**: david.jenkins@suttonacademy.attrust.org.uk
Internet Filtering	**Software**: PaloAlto Firewall	**Last Updated**:
Internet Monitoring	**Software**: eSafe & Impero	**Last Updated**:
Email Filtering	**Software**: Microsoft Office 365	**Last Updated**:
Email Monitoring	**Software**: eSafe & Impero	**Last Updated**:
Curriculum Map	**Owner**: Nicky Elvidge	**Stored**:
E-Safety Training Plan	**Owner**: Dave Jenkins	**Stored**:
E-Safety & Acceptable Use Policy - Pupils	**Owner**: Rebecca Hollett	**Stored**:
E-Safety & Acceptable Use Policy - Staff	**Owner**: Claire Thorpe	**Stored**:
Permission slips for digital display – images (website)	**Owner**: Rebecca Hollett	**Stored**:
Incident Log and Reporting Process	**Owner**: Dave Jenkins	**Stored**:
Risk Assessment and Log	**Owner**: Dave Jenkins	**Stored**:
Reporting facility for users (website/incidents)	**Owner**: Dave Jenkins	**Location**:
A system in place to provide reports of websites visited	**Owner**: eSafe & Impero	**Stored**: Esafe External Impero Local DC1

Appendix 2

Staff and Volunteers Acceptable Use Policy

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times. Within ATT, e-safety is the responsibility of everyone. As such all staff and volunteers should promote positive safety messages in all uses of ICT whether with other members of staff or with pupils.

This Acceptable Use Policy is intended to ensure that:

- Staff and volunteers will act responsibly to stay safe while online, being a good role model for younger users.
- Effective processes and procedures are in place for the online safety of all users and the security of devices, systems, images, personal devices and data.
- Staff and volunteers are aware of, and can protect themselves from, potential risk in their use of online technologies.

For my professional and personal safety, I understand that:

- I will ensure that my online activity, including the use of social networking sites does not compromise my professional responsibilities, nor bring the Trust or academy into disrepute
- My use of technology, including the internet and software, will be monitored through academy systems
- I will not use technology provided by the academy for personal business (including emails) unless permission has been given by the Principal
- I will not use personal ICT equipment for professional purposes unless a risk assessment has been carried out by the E-Safety Officer and the E-Safety Officer has granted permission and use is therefore agreed.

Communication

- When communicating professionally, I will use technology provided by the academy e.g. not using personal email addresses, mobile phones, (unless checked and agreed by the E-Safety Officer, see above) or social media logins for work related communications.
- I am aware that academy data, including emails, is subject to the ATT Freedom of Information Policy and will therefore ensure that all communications are kept professional.
- I will ensure that all communications on behalf of ATT or the academy to external organisations are professionals and where I am unsure of suitability of content I will seek advice from my line manager. I understand that I am responsible for the content that I send.

The Network

- I will not disclose my login username and password to anyone. I understand that there is no occasion when a password needs to be shared with another member of staff, pupils or ICT Support.

- I will change my password regularly.
- I will not allow pupils or colleagues access to my personal logon rights to any academy information system (e.g. MIS). I understand that if I do allow pupils or colleagues access it could lead to a breach of the Data Protection Policy and network security.
- I will log off the network or lock my computer and check that the logging off procedure is complete before leaving my computer.

For the safety of others

- I will not copy, remove or otherwise alter any other user's files, without authorisation.
- I will share the personal data of others only with their permission.

Images and Videos

- I will not upload onto the internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in the academy) and personally (e.g. staff outings).
- I will not store images and videos of pupils on a personal device.

Virus and other Malware

- I will report any virus outbreaks to ICT Support as soon as is practical to do so, along with the name of the virus (if known) and the actions taken.

For the safety of ATT

- I will not deliberately bypass any systems designed to keep the academy safe.

Internet access

- I will not intentionally access or attempt to access anything illegal, harmful or inappropriate, including child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting radicalisation and extremism; promoting illegal acts; and any other information that maybe offensive to colleagues.
- It is my responsibility to immediately report any illegal, harmful or inappropriate incident to the DSL or E-Safety Officer.

Social Networking

- I will not share my online personal information (e.g. social networking profiles) with the children and young people in my care. Staff using social networking for personal use should never undermine the academy (e.g. its staff, parents and/or pupils). Inappropriate use of social media during and outside of work hours could lead to disciplinary action.
- Social networking is allowed in the academy in accordance with the ATT E-Safety and Social Media Policies.
- I will not become 'friends' with academy parents or pupils on social networks, unless a pre-existing relationship exists (e.g. niece, nephew etc.).

Data Protection

- I will only transport, hold, disclose or share personal information about myself and others, as outlined in the ATT Data Protection Policy. Where personal data is transferred externally, it must be encrypted.
- I understand that the ATT Data Protection Policy requires that any personal data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by the ATT Data Protection Policy to disclose such information to an appropriate authority.
- If it is necessary for me to take work home, or offsite, I will ensure that my device (laptop, USB, pen drive etc.) is encrypted or the data is kept securely in Office 365 (SharePoint or OneDrive for Business). I understand that under no circumstances should data concerning personal information be taken offsite on an unencrypted device.

I confirm that:

- I have read and agree to abide by the Staff and Volunteers Acceptable Use Policy.
- I have read and understand the ATT E-Safety and Social Media Policies.
- I understand that breaches of the Staff and Volunteers Acceptable Use Policy are subject to disciplinary action under the ATT Disciplinary Procedure.

If you are unsure about responding to any of the above statements, please contact your academy E-Safety Office or James Howell, ATT's IT Manager.

Name: _____

Signature: _____

Date: _____

Appendix 3

Acceptable Use Policy for Pupils (KS2 or above)

Background

Technology is a part of learning, entertainment and communication however the use of technology can also bring risks. It is important that you learn to recognise risks and take action to stay safe. When using technology within the academy, you must agree to the following:

I understand that my internet and email activity is subject to monitoring.

I promise to only use the academy ICT for schoolwork that the teacher or responsible adult in school has asked me to do.
I promise not to look for or show other people things that may be offensive or distressing.
I promise to show respect for the work that other people have done.

I will not use other people's work or pictures without permission to do so.
I will not damage the ICT equipment. If I accidentally damage something I will tell my teacher.
I will not share my password with anybody. If I forget my password I will let my teacher know.
I will not use other people's usernames or passwords.
I will not share personal information online with anyone.
I will not download anything from the internet unless my teacher has asked me to.
I will not try to access anything illegal.
I will not sign up to and use social networking sites I am not permitted to.
I will not access or share any sites or information that may cause offence or harm to me or others.

I will let my teacher or responsible adult in school know if anybody asks me for personal information.
I will be polite and responsible when I communicate with others.
I will only use my personal device if I have received permission from a member of staff.
I will let my teacher or responsible adult in school know if anybody says or does anything to me that is hurtful or upsets me.
I will let my teacher or responsible adult in school know if someone has accessed or shared a website or information that is offensive or illegal.
I will be respectful to everybody online. I will treat everybody the way that I want to be treated.

I understand that some people on the internet are not who they say they are and some people may be unkind and wish me harm. I will tell my teacher if I am ever concerned in the academy or my parents if I am at home.
I understand that I am responsible for my actions and the consequences. If I break the rules in the Acceptable Use Policy there will be consequences of my actions and my parents will be told.
I understand that my use of academy technology systems and devices is monitored when I am working both on and offline.

I have read and understood the above and agree to follow these guidelines.

Name of Pupil: _____

Signed: _____

Year Group: _____

Date: _____

I have read this Acceptable Use Policy and understand that my child's internet access could be monitored to ensure that there is no illegal or inappropriate activity by any user of the academy network. I acknowledge that this has been explained to my child and that they have had the opportunity to voice their opinion and to ask questions.

Name of Parent: _____

Signed: _____

Date: _____

Appendix 4

Acceptable Use Policy for Pupils (KS1 and below)

Background
Technology is a part of learning, entertainment and communication however the use of technology can also bring risks. It is important that all children learn to recognise risks and take action to stay safe. When using technology within the academy, they must agree to the following rules:

I will ask an adult if I want to use the computer.
I will only use activities that an adult has told or allowed me to use.
I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
I will tell an adult if I see something that upsets me on the screen.

I know that if I break the rules I might not be allowed to use the computer.
I know that my use of computers is checked.

I agree to follow the rules for using a computer.

Name of Pupil: _____

Signed: _____

Date: _____

I acknowledge that the rules have been explained to my child and that they have had the opportunity to voice their opinion and to ask questions.

Name of Parent: _____

Signed: _____

Date: _____

Appendix 5

Academy Specific Procedures

Personal devices are classed as the following:

- Mobile phones
- Tablets
- Laptops.

The ATT E-Safety Policy states that personal devices can be used at the discretion of each academy. The E-Safety Officer must ensure that the device is safe to use and follows the filtering and monitoring policies within the academy. In some settings, such as Nursery and Early Years, personal devices are not permitted. Local procedures should be identified and followed.

(3.4) **Mobile phones and hand-held electronic devices**: pupils may only use mobile phones and wireless hand-held devices if specifically asked to by a member of staff and in line with the academy policy for the use of mobile phones (Appendix 5). Staff should ensure they follow academy policy on the use of mobile phones and in line with the following:

- Mobile phones should only be answered and in sight of administration areas of the building. Classroom based staff should store their mobile phones in a safe place away from the setting and should not access them in lesson and extra-curricular time. It is recommended that mobile phones are password protected and insured.
- Visitors, including Trust staff, contractors and parents/carers should be made aware of the **NO USE** policy on entry to the academy and through reminders such as posters and verbal reinforcement by members of staff accompanying them. Any photography required of the building (e.g. for estates purposes) should be completed when children are not present. Academy staff should challenge any use of mobile phones that does not adhere to this policy.

The academy approach to the use of personal devices is provided here: [Please add details in this box]:

Appendix 6
Useful References

Keeping Children Safe in Education (September 2016)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/550511/Keeping_children_safe_in_education.pdf

ATT advice and Guidance: Protecting our children and young people from Radicalisation and Extremism

ATT Safeguarding Policy, Procedure and Best Practice

E-Safety Advisor: useful advice and guidance to schools, pupils and parents
http://www.esafety-adviser.com/

Thinkuknow: Guidance from Child Exploitation and Online Protection Centre (CEOP)
https://www.thinkuknow.co.uk/

Kidsmart: E-Safety information and guidance
http://www.childnet.com/resources/be-smart-on-the-internet

Safer Internet Day Official Website: Information, resources and activities for Safer Internet Day
https://www.saferinternet.org.uk/safer-internet-day

Sexting in schools and colleges: **Responding to incidents and safeguarding young peopl**e, UKCCIS 2016
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609874/6_2939_SP_NCA_Sexting_In_Schools_FINAL_Update_Jan17.pdf

Growing up Digital, A report of the Growing up Digital taskforce (January 2017)
https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Growing-Up-Digital-Taskforce-Report-January-2017_0.pdf