e-Safety Policy

Bristnall Hall Academy

Policy reviewed by Academy Transformation Trust on	July 2014
Policy adopted by Local Governing Body on	23/09/2014

This policy links to:	***Located***
• Freedom of Information Policy • Data Protection Policy • Disciplinary Procedure • Behaviour Policy • Social Media Policy	All Policies can be acc

REVIEW DATE: July 2016

Content

1 Background 3
2 Roles & Responsibilities 4
3 Technology 6
4 Safe Use 7
5 Trust and academy websites 8
6 Useful websites for reference and resources 9
Appendix 1 - Staff and Volunteers Acceptable Use Policy 10
Appendix 2 - Acceptable Use Policy for Pupils (KS2 and above) 13
Appendix 3 - Acceptable Use Policy for Pupils (KS1 and below) 15

ESafety Record Sheet

e-Safety Officer	Name: Phillip Wakeman	Contact Details: Bristnall Hall Academy, 0121 552 2545
Technical Support lead	Name: Phillip Wakeman	Contact Details: Bristnall Hall Academy, 0121 552 2545
Governor responsible for e-Safety (Safeguarding Link Governor)	Name: S Tilsley	Contact Details:
Internet Filtering	Software: Cyberoam hardware appliance	Last Updated: Cyberoam hardware appliance
Email Filtering	Software: Cyberoam hardware appliance	Last Updated: Cyberoam hardware appliance
e-Safety training Plan	Owner: P Wakeman	Stored:
e-Safety and Acceptable Use Policy - Pupil responses	Owner : School Office	Stored: School Office
e-Safety and Acceptable Use Policy – Staff responses	Owner : P Wakeman	Stored: IT Office
Permission Slips for digital display of pupils images e.g. on academy website	Owner: School Office	Stored: School Office
Incident Log & reporting process	Owner : P Wakeman	Stored: IT Office
Risk Assessment and Log	Owner : P Wakeman	Stored: IT Office

1 Background

1.1 Safeguarding is a serious matter; at our academies we 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.

1.2 We have duty of care to ensure that all our pupils are competent, informed safe users of ICT and web based resources. Understanding 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.

1.3 The purpose of this policy is:

- to empower the whole Trust 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.

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

1.5 At the start of each academic year, or on induction if part way through a year, staff and volunteers will sign the Staff and Volunteers Acceptable Use Policy (appendix 1). 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 the revised e-Safety Policy.

1.6 All pupils and parents will sign a copy of the appropriate Pupil's Acceptable Use Policy (appendices 2 and 3) 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's Acceptable Use Policy each academic year. On entry into a secondary academy parents and pupils will be required to sign and return a copy of the appropriate Pupil's Acceptable Use Policy. Pupils in KS3, KS4 or KS5 are then required to revisit the Pupil's Acceptable Use Policy annually and the academy is responsible for evidencing that this has occurred. Upon signing the Acceptable Use Policy, pupils will be permitted access to academy technology including the internet.

2 Roles & Responsibilities

Academy Transformation Trust

2.1 The Trust will:

- Review this policy annually and in response to any e-safety incident to ensure that the policy is up to date.

Local Governing Body

2.2 The local governing body will:

- Ensure all aspects of technology within the academy meet the e-safety requirements within this policy
- Ensure safety incidents are properly dealt with and ensure policies and procedures are effective in managing those incidents.
- 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 through technology use
    - Receive regular updates from the Principal in regards to training, identified risks and incidents
    - Advise on changes to the policy
    - Establish the effectiveness of e-safety training within the academy
    - Recommend further initiatives for e-safety training and awareness within the academy.

Principal

2.3 The Principal has 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. Responsibility for the technical elements of e-safety should be delegated to a member of support staff. The Senior Leader with responsibility for e-Safety (or Principal if a Senior Leader is not nominated) will be known as the e-Safety Officer for the purposes of this policy. 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. The Principal will ensure that:

- e-safety training throughout the academy is planned and up to date and appropriate to the recipient i.e. pupils, all staff, senior leadership team, Local Governing Body, and parents
- The e-Safety Officer has appropriate CPD to undertake their duties e.g. CEOP training
- Annual e-safety training is arranged for all staff
- All e-safety incidents are dealt with appropriately, promptly and a record kept including details of the incident and action taken.

e-Safety Officer

2.4 The e-Safety Officer as named will:

- Keep up to date with the latest risks to children whilst using technology
- Review the policy regularly and bring any matters to the attention of the Principal
- Advise the Principal on e-safety matters
- Engage with parents and the academy community on e-safety matters within the academy and/or at home
- Liaise with the with ICT support and other agencies as required
- Keep a log of all e-safety incidents; ensure staff know what to report and ensure appropriate audit trail
- Ensure technical safety measures within the academy are fit-for-purpose(e.g. Internet filtering software; behaviour management software)
- Ensure appropriate reporting procedures are in place e.g. from reporting function of internet filtering software.

ICT Support

2.5 ICT Support is responsible for ensuring that the ICT technical infrastructure is secure; this will include the following:

- Anti-virus is fit-for-purpose, up to date and applied to all capable devices
- Operating system up dates are regularly monitored and devices updated as appropriate
- Any e-safety technical solutions such as internet filtering are operating correctly
- Filtering levels are applied appropriately and according 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 changed regularly. Passwords should be a minimum of eight characters for staff and secondary age pupils.
- The Administrator password is to be changed termly.

All Staff

2.6 Staff to ensure that:

- They have signed the Acceptable Use Policy.
- All details within this policy are understood, any uncertainty should be discussed with the e-Safety Officer and /or Principal
- Any e-safety incident is reported to the e-Safety Officer, or the Principal in their absence, and an incident report is made
- Promoting and sharing e-safety practices planned for and embedded into curriculum practices
- E-safety training is undertaken annually.

All Pupils

2.7 The boundaries of use of ICT equipment and services in this academy are given in the Pupils Acceptable Use Policy; any deviation or misuse of ICT equipment or services will be dealt with in accordance with the Behaviour Policy.

2.8 E-safety is embedded into our curriculum; pupils will be given appropriate advice and guidance by staff. Pupils will be fully aware how they can report areas of concern within or outside the academy.

Parents and Carers

2.9 Parents play the most important role in the development of their children; as such the academy will support parents 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 up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure children are empowered.

2.10 Parents must also understand the academy needs to have procedures in place to ensure that their child can be properly safeguarded. As such parents will receive a copy of the Pupil Acceptable Use Policy. Parents should support the academy when sanctioning pupils for compromising the e-safety of themselves or others.

3 Technology

3.1 The academy uses a range of ICT devices. In order to safeguard the pupils and prevent loss of personal data we employ the following assistive technology:

- **Internet Filtering** – we use software to prevent access to illegal websites. It also prevents access to inappropriate websites; 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. 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.
- **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.
- **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 (i.e. loss/theft of device such as 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 termly basis, or if there has been a compromise whichever is sooner. 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.

4 Safe Use

4.1 ***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 signing the appropriate Acceptable Use Policy.

4.2 ***Email*** – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly the use of personal email addresses for work purposes is not permitted. Pupils are permitted to use the email system and as such will be given their own email address.

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

4.4 ***Mobile phones and hand-held electronic devices*** - must be switched off and remain in the pupil's bags at all times while onsite. Pupils may only use mobile phones if specifically asked to do so by a member of staff. Wireless hand-held devices should not be brought into the academy and should not be used to access the internet while on the academy site. Mobile phones and hand-held devices will be confiscated if seen and only released to a parent or adult carer.

4.5 ***Sexting*** - is becoming more common. Sexting is described as the "generation of video and/or images that are indecent or of a sexual nature by children under the age of 18." We will ensure secondary pupils are taught the legal, social and moral issues around sexting. Pupils will be encouraged to report all incidents of sexting. Teaching staff will inform the Designated Officer for Child Protection who will act according to the Child Protection Policy and the guidance outlined in the "Sexting" in schools: advice and support around self-generated images 2013 document.

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

4.7 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.

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

4.9 ***Incidents*** – any e-safety incident is to be brought to the immediate attention of the e-Safety Officer, or in his/her absence the Principal. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

4.10 ***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. 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.

4.11 e-safety for pupils is embedded into the curriculum; whenever 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.

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

4.13 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.

5 Trust and academy websites

5.1 The ethos of The Trust 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.

Permission will be obtained for use of images on websites before any images of videos are used on The Trust or academy website.

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

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

6 Useful websites for reference and resources

esafety-adviser.com – useful advice and guidance to schools, pupils and parents
safesocialnetworking.org - provides resources for young people
thinkuknow.co.uk – guidance from the Child Exploitation and Online Protection Centre (CEOP)
kidsmart.org.uk - e-Safety information and guidance
saferinternet.org.uk – resources and activities and focus on safer internet day

Appendix 1 - 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 The Trust e-safety is the responsibility of everyone. As such all staff and volunteers should promote positive safety messages in all use 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 systems 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 on-line activity does not compromise my professional responsibilities, nor bring The Trust or academy into disrepute
- My use of technology could be monitored
- 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.

Communication

- When communicating professionally I will use technology provided by the academy (i.e. not using personal e-mail addresses, mobile phones or social media logins for work related communications).
- I am aware that academy data, including emails, is subject to the Freedom of Information Policy and will therefore ensure that all communications are kept professional.
- I will ensure that all communications on behalf of The Trust or academy to external organisations have been agreed by my line manager.

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 log on 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 a computer.

For the safety of others:

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

Images and Videos

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

Viruses 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 The Trust:

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

Internet Access

- I will not 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 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 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.
- Social networking is allowed in the academy in accordance with the e-Safety and Social Media Policy only. Staff using social networking for personal use should never undermine the academy its staff, parents of pupils. Overuse of personal social media during work hours could lead to disciplinary action. Staff should not become 'friends' with parents or pupils on social networks.

Data Protection

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy. Where personal data is transferred externally, it must be encrypted.
- I understand that the Data Protection Policy requires that any personal datat 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 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. 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 e-Safety Policy
- I understand that breaches of the Staff and Volunteers Acceptable Use Policy are subject to disciplinary action under the Disciplinary Procedure.

Name:_____

Signature: _____ Date: _____

Appendix 2 - Acceptable Use Policy for Pupils (KS2 and 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 has asked me to do
I Promise – not to look for or show other people things that may be upsetting
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 – let my teacher 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 know if anybody says or does anything to me that is hurtful or upsets me
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 can be nasty. 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 action and the consequences. If I break the rules in this Acceptable Use Agreement there will be consequences of my actions and my parents will be told.

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

Name (pupil): _____ Signed:_____

Year Group: _____ Date: _____

I have read this Acceptable Use Agreement 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: _____

Signed (Parent): _____ Date: _____

Appendix 3 - 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 a computer.

I agree to follow the rules for using a computer.

Name: _____

Signed (Child): _____ 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: _____

Signed (Parent): _____ Date: _____