Acorn Trust Online Safety Policy

ACORN TRUST

Sowing Seeds for a Brighter Future

Written by:	A Burkes
Date agreed:	Feb 2019
Next Review Date:	Spring 2020
CEO Signature	

Mission Statement

The Acorn Trust is a Multi-Academy Trust established with the aim of providing outstanding learning and opportunities for the children within its care.

Children are our nation’s most precious resource. Their school life and learning experience will shape them for the whole of their lives

Safeguarding Statement

At the Acorn Trust we recognise our moral and statutory responsibility to safeguard and promote the welfare of all children.

We work to provide a safe and welcoming environment where children are respected and valued. We are alert to the signs of abuse and neglect and follow our procedures to ensure that children receive effective support, protection and justice.

The procedures contained in the Safeguarding Policy apply to all staff, volunteers and governors

Online safety Policy

Statement of intent

At the Acorn Trust we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use.

Our Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The Trust is committed to providing a safe learning and teaching environments for all pupils and staff, and has implemented important controls to prevent any harmful risks.

This policy will operate in conjunction with other important policies in our Academy Trust, including our Anti-bullying Policy, Data Protection Policy, Child Protection and Safeguarding Policy, and Allegations against Staff Policy.

1. Legal framework

1.1. This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspection Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Safer Working Practice (October 2015)
- Keeping Children Safe in Education: for schools and colleges (Sept 2018)
- Acorn Trust 'General Data Protection Regulations' Policy.

2. Use of the internet

2.1. The Acorn Trust understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for schools within the Trust to implement, which minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff, due to inappropriate internet access or use both inside and outside of school and to deal with incidents of such as a priority.

3.2. The online safety officers, (usually the Headteacher and/or Pastoral Manager and/or Computing Lead), is responsible for ensuring the day-to-day online safety in school and managing any issues.

3.3. The Headteacher is responsible for ensuring that the online safety officers and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

3.4. The online safety officers will arrange or provide all relevant training and advice for members of staff on online safety.

3.5. The Headteacher will ensure there is a system in place which monitors and supports the online safety officers, whose role is to carry out the monitoring of online safety in the school.

3.6. The online safety officers will regularly monitor the provision of online safety, in the school and return this to the Headteacher.

3.7. Employees must report incidents and inappropriate internet use, either by pupils or staff to the Headteacher. This will also be recorded on Impero system within school.

3.8. Cyber bullying incidents will be reported in accordance with the Trust's Anti-Bullying Policy.

3.9. The online safety officers will ensure that all members of staff are aware of the procedure when reporting online safety incidents, and will keep a log of all incidents recorded.

3.10. The governor for safeguarding will hold regular meetings with the online safety officers to discuss the effectiveness of the online safety provision, current issues, and to review incident logs. A written online safety report is shared with each school's governing body each term.

3.11. The Directors will evaluate and review this Online safety Policy on an annual basis.

3.12. The Trust will review and amend this policy with the online safety officers, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

3.13. Teaching staff are responsible for ensuring that online safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.14. All staff are responsible for ensuring they are up-to-date with current online safety issues, and this Online safety Policy.

3.15. All staff and pupils will ensure they understand and adhere to the Acceptable Usage of IT Policy, which they must sign and return to the Headteacher. (Appendix 3)

3.16. Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

3.17. The Headteacher and online safety officers are responsible for communicating with parents regularly and updating them on current online safety issues and control measures through the school website, newsletters and parental meetings/workshops. (See Appendix 1 for links and resources).

4. Online safety control measures

4.1. Educating pupils:

- An online safety programme will be established and taught across the curriculum on a regular basis, ensuring pupils are aware of the safe use of new technology both inside and outside of the school.
- Pupils will be taught about the importance of online safety and are encouraged to be critically aware of the content they access online.
- Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be presented in all classrooms.
- Pupils are instructed to report any suspicious use of the internet and digital devices.
- Pupils will be taught how to minimise screens (rather than shutting down) and informing the teacher if offending data is obtained, so the teacher can investigate.
- See Appendix 1 for resources and links

4.2. Educating staff:

- All staff will undergo online safety and safer working practice training on an annual basis to ensure they are aware of current online safety issues and any changes to the provision of online safety.
- All staff will undergo regular audits by the online safety officers in order to identify areas of training need.

- All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.
- Any new staff are required to read the Online safety policy, Acceptable Usage and Social Media Policy as part of their induction programme, ensuring they fully understand them – and sign any acceptable usage policies as required.

4.3. Internet access:

- Internet access will be authorised once parents and pupils have returned the signed consent form as part of the Acceptable Use Policy.
- A record will be kept in the school office of all pupils who have been granted internet access.
- All users in *Year 2* and above will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other pupils using their login details.
- Pupils' passwords will be changed on a regular basis, and their activity is continuously monitored by the online safety officers and the schools' on-line security system, Impero.
- Management systems are in place to allow teachers and members of staff to control workstations and monitor pupils' activity. Impero is used to support schools in this. Impero is used to address esafety and monitor the safe use of computers, on and offline. This helps to identify safeguarding risks from the words that are typed, even if not saved in documents. This is to help address worries that children may have by; letting them confide anonymously, resolve bullying issues, detect issues that children may be of concern to a safeguarding officer. Also built into the software are additional functions that help to save money on energy and printing costs and tools to help staff use devices as effectively as possible to prevent time being lost in lessons using ICT equipment.
- All school systems will be protected by up-to-date virus software, Sophos. Sophos provides online security for schools in the Trust. Sophos guards the schools' internet connections from threats that are posed to internet users and the network infrastructure. This helps to prevent hacking of systems and data and a wide range of malware, viruses etc. This also helps to restrict access to inappropriate web-content.
- Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the Headteacher.

- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

4.4. Email:

- Pupils and staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other pupils, staff or third parties via email.
- Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.
- Chain letters, spam and all other emails from unknown sources will be deleted without opening.

4.5. Social networking:

- This links to the Acorn Academy Trust Social Media Policy.
- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the Headteacher.
- Pupils are regularly educated on the implications of posting personal data online, outside of the school.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school / Acorn Academy Trust as a whole.
- Staff are not permitted to communicate with pupils over social networking sites.

Social networking – For schools within the Trust that use Twitter:

- Use of school Twitter accounts will be accessed only by teachers
- School Twitter accounts will only follow accounts of other classes of Bedford Hall Methodist Primary School. School Twitter accounts will not follow any other accounts.
- Twitter is blocked within school therefore teachers are only able to send tweets out of school.

- Class Twitter accounts may only be accessed on their designated school device (teacher's registered IPad).
- Class Twitter accounts will not reply to messages and therefore will not engage in any form of discussion.
- Twitter accounts may be viewed in school with pupils, teachers must check before hand to ensure no inappropriate content may be viewed in the timeline.
- Acceptable content for Twitter is news, events, pictures of children's work, children in groups, individuals (parental permission/or not will be advised by the school office). Exceptions to permission for photographs will be LAC.
- Trips will not be advertised in advance.
- Children's names will not be used in tweets; phrases such as 'Year 5..' or 'this boy..' will be used.
- School staff will be advised not to follow the school Twitter using their own personal Twitter accounts.
- Twitter passwords will be changed annually.
- Abuse must be reported to the Head Teacher immediately.
- Hashtags may not be used unless approved by the Head Teacher or SLT.
- The school will control access to social networking sites, and consider how to educate pupils in their safe use.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils will only be allowed on the learning Platform social networking sites within school.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils will be advised to use nicknames and avatars when using social networking sites. (Guidelines on this are incorporated within COMPUTING lessons).

Social networking – For schools within the Trust that use Blogging:

- Blogs that can be accessed from the Internet can potentially be read by anyone. The main eSafety consideration is therefore to ensure that pupils do not reveal any personal information about themselves, other pupils or staff that could allow a stranger to work out who they are or where they are.
- Many blogs also have the facility for visitors to add comments to posts. This could result in inappropriate comments being left by other pupils or adults, or requests for personal information. Staff

should turn comments off, or hold comments until a member of staff approves them.

- Depending on the settings of the blog, visitors to your blog may be requested to enter their name and/or email address before being able to post a comment. Pupils should not enter their personal information into any blog when leaving a comment, and staff should ensure the settings on the blog allow visitors to leave anonymous comments to avoid this.
- Schools should also consider how they will control who can post blog entries, and when. Most blogs require a username and password to be entered before entries can be made. However, if pupils are given their own username and password, they may be able to post entries from home without supervision. In particular, for younger pupils you may consider making class entries i.e. class1, year1 usernames on blogs.
- In addition, pupils should be reminded that bloggers are liable for the content of their blogs, and they should not only try and ensure any statements or facts are accurate, but also ensure they do not include statements about other people that aren't true, or are unsubstantiated.
- By default pupils must be logged in with their username and password to post a comment.
- All comments will be moderated by the class teacher or administrator before going live.
- The ability to post anonymously is turned off.
- Blogs are only added to the blogroll (index) when requested by the school.

Prevent Strategy

- The Trust's Child Protection and Safeguarding policy should be followed if a concern is raised regarding internet or social networking activity which links to extremism or radicalisation, in line with the government's Prevent Strategy.
- If a reported incident involved a member of staff, the Headteacher will deal with such incidents in accordance with the Trust's Allegations against Staff Policy.
- The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.
- The government's Prevent Strategy can be found at the following address: https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

- See Appendix 1 for links and resources

4.6. Published content on the school's website and images:

- The Headteacher will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- The only contact details on the school's website will be the telephone number, email and address of the school. No personal details of staff or pupils will be published.
- Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Pupils and parents are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with the school's policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.

4.7. Mobile devices:

- Please see the Acorn Academy Trust's Mobile Phone Usage Policy.
- Please see the Acorn Academy Trust's Staff Acceptable Usage Policy.
- Please see the IPAD Acceptable Use Policy Guidelines (see Appendix 2). This should be completed as part of teaching staff Induction.

5. Cyber bullying

5.1. For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.

5.2. The Trust recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

5.3. The Trust will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

5.4. The Trust will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

5.5. The Trust has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with the Acorn Trust Anti-Bullying Policy.

5.6. The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

6. Reporting misuse

6.1. Misuse by pupils:

- Teachers have the power to discipline pupils (following the school's Behaviour Policy) who engage in misbehaviour with regards to internet use. However, more serious incidents will be directly dealt with by the Headteacher.
- All parent/carers will share the Acceptable Use Agreement (Appendix 3) at the start of each school year with their child and complete a slip to say they have read it.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the Headteacher in written form.
- Any pupil who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Complaints of a child protection nature shall be dealt with in accordance with the Trust's Child Protection and Safeguarding Policy.

6.2. Misuse by staff:

- Any misuse of the internet by a member of staff should be immediately reported to the Headteacher.
- The Headteacher will deal with such incidents in accordance with the Trust's Allegations against Staff Policy, and may decide to take disciplinary action against the member of staff.
- The Headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

Appendix 1:

Useful resources for teachers

www.net-aware.org.uk/

BBC Stay Safe - www.bbc.co.uk/cbbc/help/safesurfing/

Becta - http://schools.becta.org.uk/index.php?section=is

Chat Danger - www.chatdanger.com/

Child Exploitation and Online Protection Centre - www.ceop.gov.uk/

Childnet - www.childnet-int.org/

Cyber Café - http://thinkuknow.co.uk/8_10/cybercafe/cafe/base.aspx

Digizen - www.digizen.org/

Kent online safety Policy and Guidance, Posters etc.

www.clusterweb.org.uk/kcn/online safety_home.cfm

Kidsmart - www.kidsmart.org.uk/

Kent Police – online safety - www.kent.police.uk/Advice/Internet%20Safety/online safety%20for%20teacher.html

Think U Know - www.thinkuknow.co.uk/

Safer Children in the Digital World www.dfes.gov.uk/byronreview/

Useful resources for parents

Care for the family - www.careforthefamily.org.uk/pdf/supportnet/InternetSafety.pdf

Childnet International "Know It All" CD

http://publications.teachernet.gov.uk

Family Online Safe Institute - www.fosi.org

Internet Watch Foundation - www.iwf.org.uk

Kent leaflet for parents: Children, COMPUTING & online safety

www.kented.org.uk/ngfl/Computing/safety.htm

Parents Centre - www.parentscentre.gov.uk

Internet Safety Zone - www.internetsafetyzone.com

Keeping Children Safe in Education: for schools and colleges (Sept 2018)

Parents’ Guide to Social Media – www.gov.uk/government/uploads/system/uploads/attachment_data/file/490001/Social_Media_Guidance_UKCCIS_Final_18122015.pdf.pdf

Parents’ Pages on Thinkuknow – www.thinkyouknow.co.uk/parents/

Prevent

Helpline for Radicalisation concerns 020 7340 7264
counter.extremism@education.gsi.go.uk

See it Report it – www.seeitreportit.org

Home Office – Report online terrorism materials – www.gov.uk/report-terrorism

Guide to safety on social networks – www.saferinternet.org.uk/advice-and0resources/parents-and-carers/safety-tools-on-online-services/social-networks

Appendix 2

Acorn Academy Trust Schools'

IPAD Acceptable Use Policy Guidelines

______________________ Employee's name

The Apple IPAD that you will be issued is the property of XXXX School, and is made available to you as a tool for teaching. To maintain the utmost professional use of this equipment, all teachers must abide by the following guidelines.

- The IPAD will only be used by myself and not shared with friends or other family members.
- I am responsible for knowing how to properly operate and protect the IPAD. *The IPAD is sensitive to moisture and extreme temperatures. The IPAD must* ***not*** *be left in a car or location where it can be damaged by cold or heat and must be kept dry and away from sources of water.*

  Clean the screen with a soft, dry cloth or anti-static cloth made for this use.

  To extend the battery life of the IPAD, do not constantly charge it. It is best to let the battery drain before recharging.

- In the event of damage or theft of the IPAD, I will report the incident within 24 hours.
- I will ensure that the IPAD is password protected and will not share this passcode with others.
- I will keep the IPAD in a locked closet or desk when not in use.
- I am responsible for understanding and adhering to all copyright requirements and district policies related to digital media and the use of this IPAD.
- Students are to be supervised by an adult when using the IPAD.
- Any **paid** apps must be approved by SLT from the school ITunes account. Free apps may be downloaded, but should be educational in nature or for appropriate reinforcement.
- I will not download any information/images from the IPAD to my personal PC. Photographs must be downloaded onto the school network and deleted from the IPAD as soon as possible.
- Photographs taken on the IPAD will be for school purpose only and cannot be used for personal photography.
- I understand that this IPAD will be subject to a regular inspection.
- I will return the IPAD to XXXXXX Primary School, upon completion of the school year for updates and routine maintenance or on leaving my position at the school.

I have read, understand, and agree to all the responsibilities as outlined in the IPAD agreement guidelines.

IPAD Model/Serial Number

Accessories issued

Employee Signature

Date

Written By J.Murphy   Reviewed and approved   September xxx
Revised by A Burkes

Appendix 3

Acorn Academy Trust

ACORN TRUST

Sowing Seeds for a Brighter Future

Acceptable Use Agreement

Primary Pupils

ACORN TRUST ACADEMY

Sowing Seeds for a Brighter Future

Agreement/Online safety rules

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for school work and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by e-mail or in a chat room, unless my parent, guardian or teacher has given my permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.

ACORN TRUST
ACADEMY
Sowing Seeds for a Brighter Future

XXXXX Primary School
Address

Dear Parent/Carer

The use of ICT including the internet, e-mail, mobile, social networking etc. has become a crucial part of learning and we want all pupils to be safe and responsible while using these valuable resources.

Please discuss these online safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact XXXX, Headteacher.

✂

Parent/carer signature

We have discussed this and …………………………………………..........(child's name) agrees to follow the online safety rules and to support the safe use of ICT at XXXXX XXX Primary School.

Parent/Carer signature …….…………………..……………………………………….

Child's class ………………………………… Date ………………………………