ASTON ALL SAINTS C OF E PRIMARY SCHOOL

eSafeguarding Policy

Date: November 2017
Review Date: 2019-20

At Aston C of E, we feel that the Internet and other technologies have an important role in the learning and teaching process and support achievements in all areas of their life while in education and beyond into adulthood. Aston C of E is committed to providing all children with opportunities to develop their ICT knowledge, skills and understanding confidently, competently and safely in their learning and in everyday contexts. Children are encouraged to become independent and astute users of technology, recognising both opportunities and risks and using strategies to stay safe and this eSafeguarding policy reflects the school's commitment to their safeguarding and well-being.

Introduction
We believe that eSafeguarding is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Leadership Team
• Develop and promote an eSafeguarding culture within the school community.
• Support the eSafeguarding coordinator in their work.
• Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafeguarding effectively.
• Regularly review the eSafeguarding incident log and be aware of the procedure to be followed should an eSafeguarding incident occur in school.
• Take ultimate responsibility for the eSafeguarding of the school community.

Responsibilities of the eSafeguarding Coordinator
• Promote an awareness and commitment to eSafeguarding throughout the school.
• Be the first point of contact in school on all eSafeguarding matters.
• Create and maintain eSafeguarding policies and procedures.
• Develop an understanding of current eSafeguarding issues, guidance and appropriate legislation.
• Ensure all members of staff receive an appropriate level of training in eSafeguarding issues.
• Ensure that eSafeguarding education is embedded across the curriculum.
• Ensure that eSafeguarding is promoted to parents and carers via the website and in response to current events or issues.
• Liaise with the local authority, the local safeguarding children's board and other relevant agencies as appropriate.
• Monitor and report on eSafeguarding issues to the leadership team and governors as appropriate.
• Ensure an eSafeguarding incident log is kept up-to-date.

Responsibilities of Teachers and Support Staff

• Read, understand and help promote the school's eSafeguarding policies and guidance.
• Read, understand and adhere to the school staff Acceptable Use Policy (AUP).
• Develop and maintain an awareness of current eSafeguarding issues and guidance.
• Model safe and responsible behaviours in your own use of technology.
• Embed eSafeguarding messages in learning activities where appropriate.
• Supervise pupils carefully when engaged in learning activities involving technology.
• **All pupils** working in the IT suite must be supervised by an adult at all times.
• Be aware of what to do if an eSafeguarding incident occurs.
• Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilties of Technical Staff

• Support the school in providing a safe technical infrastructure to support learning and teaching.
• Take responsibility for the security of the school ICT system.
• Report any eSafeguarding-related issues that come to your attention to the eSafeguarding coordinator.
• Develop and maintain an awareness of current eSafeguarding issues, legislation and guidance
relevant to your work.
• Liaise with the local authority and others on technical issues.
• Maintain a professional level of conduct in their personal use of technology at all times.

Responsibilities of Pupils

• Read, understand and adhere to the school pupil Acceptable Use Policy (AUP).
• Help and support the school in creating eSafeguarding policies and practices; and adhere to
any policies and practices the school creates.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
• Take responsibility for your own and each others' safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
• Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
• Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
• Discuss eSafeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

• Help and support school in promoting eSafeguarding.
• Read, understand and promote the school pupil Acceptable Use Policy (AUP) with your children.
• Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
• Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies

• Discuss eSafeguarding concerns with your children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using it.
• Use any eSafeguarding links on the school website.
• Model safe and responsible behaviours in your own use of technology.
• Consult with the school if you have any concerns about your children's use of technology.

Responsibilities of Governing Body
• Read, understand, contribute to and help promote the school's eSafeguarding policies and guidance.
• Develop an overview of the benefits and risks of the Internet and common technologies used by pupils.
• Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
• Develop an overview of how the school encourages pupils to adopt safe and responsible behaviours in their use of technology in and out of school.
• Support the work of the school in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in eSafeguarding activities.
• Ensure appropriate funding and resources are available for the school to implement their eSafeguarding strategy.

Responsibilities of any Adult or Community Education Training Staff
• Develop and promote an eSafeguarding culture within the school community.
• Support the eSafeguarding coordinator in their work.
• Make appropriate resources, training and support available to members of the school community to ensure they are able to carry out their roles with regard to eSafeguarding effectively.
• Read, understand and help promote the school's eSafeguarding policies and guidance.
• Read, understand and adhere to the school staff and other adults ACCEPTABLE USE POLICY (AUP).
• Develop and maintain an awareness of current eSafeguarding issues and guidance.
• Model safe and responsible behaviours in your own use of technology.
• Embed eSafeguarding messages in learning activities where appropriate.
• Supervise students carefully when engaged in learning activities involving technology.
• Be aware of what to do if an eSafeguarding incident occurs.
• Maintain a professional level of conduct in their personal use of technology at all times.

Learning and Teaching
We believe that the key to developing safe and responsible behaviours online, not only for pupils but everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to safely benefit from the opportunities the Internet brings.
• We will provide a series of specific eSafeguarding-related lessons in every year group as part of the ICT curriculum and other lessons.
• We will celebrate and promote eSafeguarding through whole-school and individual class activities.

• We will discuss, remind or raise relevant eSafeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
• Staff will model safe and responsible behaviour in their own use of technology during lessons.

How parents and carers will be involved
We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this we will:
• include useful links and advice on eSafeguarding regularly in newsletters and on our school website.

Managing ICT Systems and Access
Internet access is provided by the Rotherham Grid For Learning who ensures that access is a safe as possible. The school infrastructure, hardware and software are managed by XI Technologies.

• The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.
• Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
• Servers, workstations and other hardware and software will be kept updated as appropriate.
• Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.
• The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.
• All users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.
• At KS1 pupils will access the Internet using an individual log-on, which the teacher supervises. All Internet access will be by working alongside a member of staff, or if working independently a member of staff will supervise at all times.
• At KS2 pupils will access the Internet using an individual log-on, which they will keep secure. Internet access will be supervised by a member of staff.
• Members of staff will access the Internet using an individual log-on, which they will keep secure. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school Acceptable Use Policy (AUP) at all times.
• Members of staff will use only school USB drives to transfer data between school and teacher laptops.
• Members of staff will not connect any personal devices (e.g. USB drives, mobile phones, cameras) to any school equipment.
• Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff.
• The school will take all reasonable precautions to ensure that users do not access inappropriate material. However it is not possible to guarantee that access to

unsuitable material will never occur. Any incidents will be logged.
• The school will regularly audit ICT use to establish if the eSafeguarding policy is adequate and that the implementation of the eSafeguarding policy is appropriate. We will regularly review our Internet access provision, and review new methods to identify, assess and minimise risks.

Filtering Internet access
• The school uses a filtered Internet service. The filtering is provided through RGFL and is password protected.
• If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the eSafeguarding coordinator.
• If users discover a website with potentially illegal content, this should be reported immediately to the eSafeguarding coordinator. The school will report this to appropriate agencies including the filtering provider, LA and CEOP .
• The school infrastructure, hardware and software is managed by XI Technologies and the wireless network is password protected.

Learning technologies in school

	Pupils	Staff
Personal mobile phones brought into school	Allowed with permission only	Allowed
Mobile phones used in lessons	Not allowed	Not allowed
Mobile phones used outside of lessons	Not allowed	Allowed
Taking photographs or videos on personal equipment	Allowed on residential visits for personal use only.	Allowed for specific staff only when on residential visits. All photos and video to be removed on return to school.
Taking photographs or videos on school devices	Allowed	Allowed
Use of hand-held devices such as iPads, tablets, PDAs, MP3 players or personal gaming consoles	Allowed with permission.	Allowed
Use of personal email addresses in school	Not allowed	Not allowed
Use of school email address for personal correspondence	Not allowed	Not allowed
Use of online chat rooms	Not allowed	Not allowed
Use of instant messaging services	Not allowed	Not allowed
Use of blogs, wikis, podcasts	Allowed (monitored)	Allowed for school use ie when a class is on residential visit
Use of video conferencing or other online video meetings	Allowed with supervision.	Allowed (not for personal use)
Use of social networking sites	Not allowed	Not allowed

Using Email

• Staff should use approved e-mail accounts allocated to them by the school and be aware that their use of the school e-mail system will be monitored and checked.

• Staff and pupils are not permitted to access personal e-mail accounts on school devices.

• Communication between staff and pupils or members of the wider school community should be professional and related to school matters only. Contact with pupils and parents must be via the school email address only.

• Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

• We will remind pupils of safe and responsible behaviours when creating, using and

storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home.
• Digital images, video and sound will only be created using equipment provided by the school.
• Staff and pupils will follow the school policy on creating, using and storing digital resources.
• In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff or pupils involved.
• Parental permission will be sought, before any online publication of images, for all children as they join our school community.

Using blogs, video, podcasts, social networking and other ways for pupils to publish content online

We may use blogs, video, podcasts other ways to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.
• Pupils will model safe and responsible behaviour in their creation and publishing of online content. For example, pupils will be reminded not to reveal personal information which may allow someone to identify and locate them.
• Pupils and staff will not access social networking sites on school devices.
• All posts and comments on blogs will be approved before publishing.
• Staff and pupils will be encouraged to adopt similar safe and responsible behaviours in their personal use of blogs, social networking sites and other online publishing outside of school.
Staff, students and volunteers will not post comments on any social media sites about their role in school, pupils or other members of staff or respond to comments made by others.

Using mobile phones

• Personal mobile phones will not be used during lessons by pupils or staff.
• Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting pupils or parents, they should do so via school.
• Staff will not be expected to use personal mobile phones in any situation where their mobile phone number or other personal details may be revealed to a pupil or parent.

Using new technologies

• As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an eSafeguarding point of view.
• We will regularly amend the eSafeguarding policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an eSafeguarding risk.

Protecting personal data

• We will ensure personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.
• Staff will ensure they properly log-off from a computer terminal after accessing personal data.
• Staff will not remove personal or sensitive data from the school premises without permission of the head teacher, and without ensuring such data is kept secure.

The school website and other online content published by the school

• The school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.
• A generic contact e-mail address will be used for all enquiries received through the school website.
• The content of the website will be composed in such a way that individual pupils cannot be clearly identified.
• The school website will not include digital images of any children where parents have specifically asked for their exclusion.
• The school website will not include digital images of staff without prior permission.

Key Stage 1 Acceptable Use Policy

Children in KS1 will follow these rules to keep them safe

- I will make sure I take care of any school-owned ICT equipment
- I will return any school-owned ICT equipment to my teacher when I have finished using it.
- I will only use the internet when my teacher says I can.
- I will only use the school's computers for my school work.
- I will only log on as myself.
- I will turn off the monitor if I see something that I feel uncomfortable with or upsets me; then I will tell my teacher straight away.
- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not say nasty or hurtful things about any member of staff or pupil online.
- I know that my use of ICT can be checked and that my parent/carer will be contacted if a member of school staff is concerned about my safety.

Key Stage 2 Acceptable Use Policy

When using the school's ICT equipment and other information systems, children in KS2 will agree to -

- I will only go on the internet using my own username and password.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I see anything like this I will tell my teacher immediately.
- I will not try and get to any websites that the school has blocked access to.
- I will make sure I take care of any school-owned ICT equipment
- I will only use memory sticks with permission from my teacher.
- I will not install any software on school computers.
- I will return any school-owned ICT equipment to my teacher when I have finished using it.
- I know that my use of ICT can be checked and that my parent/carer contacted if a member of school staff is concerned about my safety.

Social Media

- I know that some websites and social networks have age restrictions and I should not use them unless I am old enough.
- I will not say nasty or hurtful things about any member of staff or pupil online.
- I will not give away any of my personal details (full name, age, date of birth, address etc.) or the personal details of other users in school, over the internet. This includes photographs or video images of me, other pupils or members of staff.
- I will never arrange to meet anyone I have only met online unless a trusted adult is with me.

Managing Digital Content

- I will only use school-owned equipment to create pictures, video and sound. Pictures, video and sound will not be taken without asking permission first.
- I will not publish anything online, e.g. images or pictures, without asking my teacher.

Email

- I will take care in opening any attachments sent by email. I will not open an attachment, or download a file, unless I know and trust the person who has sent it.

Mobile phones and devices

- I will only bring my mobile phone or other devices to school with permission from my teacher.

- I will hand mobile phones and mobile devices to my teacher for safe keeping during school hours and only use I when I have permission.

- I will not take pictures in school on my mobile phone or mobile device.

Agreement

The above rules and guidance will be explained to all children in school appropriate to their age and stage and will be displayed in classes and the ICT suite in a simple format. This may be presented as a charter and be a focus in an Internet Safety Week for example.

Staff Acceptable Use Policy

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

- I have read and understood the implications and my personal responsibilities in relation to the use of ICT equipment which is detailed within this policy.
- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the eSafeguarding coordinator.
- I will not share my passwords with any colleagues or pupils within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the eSafeguarding coordinator/ Headteacher.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- 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, I will report this to the network manager / eSafeguarding coordinator.
- I will ensure that all devices taken off site, (laptops, tablets, cameras, removable media or phones) will be secured in accordance with the school's Data Protection Registration and any information-handling procedures both on and off site.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will secure any equipment taken off site for school trips.
- I will only use school-owned or provided portable storage (USB sticks, portable hard drives etc).
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.

- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).

- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation.

- I will return any school-owned ICT equipment or software to the relevant individual within school once it is no longer required.

- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.

- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

- I understand that if I do not follow all statements in this AUP and in other school policies relating to the use of ICT equipment I may be subject to disciplinary action in line with the schools established disciplinary procedures.

Social Media

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Twitter and YouTube or any other online publishing websites.

- I must not use social media tools to communicate with current or former pupils under the age of 18.

- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.

- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.

- Staff must not access social networking sites for personal use during school hours.

- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the eSafeguarding coordinator.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.

- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants

will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the eSafeguarding Policy.

- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the designated member of staff. (eSafeguarding coordinator or Head Teacher).
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright law.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school website and blogs. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Learning and teaching

- I will support and promote the school eSafeguarding policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of eSafeguarding and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Email

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.

- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.

- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.

- Emails sent to external organisations will be written carefully and authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the headteacher, line manager or another suitable member of staff into the email.

- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.

- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to ‘silent’ mode during school hours.

- Bluetooth communication should be ‘hidden’ or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Leadership Team in emergency circumstances.

- I will not contact any parents or pupils on my personally-owned device.

- I will not use any personally-owned mobile device to take images, video or sound recordings without prior permission and subsequent deletion on return to school.

Agreement

I have read and understand all of the above listed points relating to my use of technology within school. I understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Staff name	
Signed	
Date	