Shorne Church of England Primary School

(A member of the Aletheia Anglican Academies Trust)

E-Safety Policy

Lead member of Staff: Ben Woodcock

Lead Governor: Luke Steggles

Date approved: October 2017

Next scheduled review: October 2019

Contents

1. Introduction

Scope of the Policy

This policy sets outlines the role of the school in ensuring that pupils are kept safe on-line in school. Although the school will take care to prevent pupils being exposed to risk while online and connected in school time, the school recognises that use of the Internet outside school is now widespread. Pupils therefore need educating as to the potential risk of using the Internet, and need to acquire skills and strategies to keep themselves safe.
This document:

- Identifies the key people and their roles and responsibilities.
- Outlines the strategy in which the school will endeavour to keep its pupils safe from harm, both by electronic protection, and by education of pupils and parents.
- Identifies the procedures to follow in the case of an incident.

2. Roles and responsibilities

2.1 E-Safety governor

The Appointed E-Safety Governor is _____. Their role includes:

- Meeting with the E-Safety Co-ordinator on a regular basis
- Regular monitoring of e-safety incident logs
- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors committee meetings

2.2 E-safety Co-ordinators

The E-Safety Coordinator is _____. Their role includes:

- Leading the school e-safety committee
- Day to day responsibility for e-safety issues with a leading role in establishing and reviewing the school e-safety policies and documentation
- Ensuring that all staff are aware of the policy and the procedures that need to be followed in the event of an e-safety incident taking place.
- Providing training and advice for staff
- To liaise with the Local Authority and other agencies if and when required
- To work with school ICT technical staff on e-safety
- To receive reports of e-safety incidents and maintain a log of incidents to inform future e-safety policy and practice
- Attends relevant meeting (committee) of Governors to inform Governors

2.3 Role of the Headteacher

The Headteacher has overall responsibility for ensuring the safety of members of the school community. However, the day-to-day responsibility for e-safety will be delegated to the E-Safety Co-ordinator. The Headteacher is also the designated person for Safeguarding.

The Headteacher will work with the E-Safety Co-ordinator drawing on each other's experience and expertise in order to ensure that pupils are kept safe, and should be aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

3. Education for children

Keeping children safe online is critically all about education. Although filters are in place to protect pupils whilst in school, this is only a small percentage of the time that a child is potentially on-line. Schools must play their part in educating children in how to negotiate the internet without the safety net of filtering in place. It is about developing risk strategies and responses to threats whether potential or real.

The School will provide E-Safety education in the following ways:

- a planned e-safety programme as part of Computing / PHSE / other lessons, with key themes regularly revisited covering all communication technologies where there is a safety risk
- key e-safety messages should be reinforced as part of a planned programme of assemblies
- children should be taught in all lessons to be critically aware that not everything they access on-line is truthful or valid and be taught to check the accuracy of information
- children should be encouraged to adopt and promote safe and responsible use of ICT, the internet and mobile devices both within and outside school
- children should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- rules for use of ICT systems and the internet will be posted in all rooms regardless of if computers are in use there, as the use of mobile devices mean that the Internet is accessible across the site
- staff should act as good role models in their use of ICT, the internet and mobile devices

4. Education for parents / carers

Educating parents is key if children are to develop strategies to deal with the potential risks of the internet. Parent's perception of risk is may be limited and/or badly informed. Scare stories in the media often cause parents unnecessary concerns, whilst obscuring real issues and risks. The school attempts to provide as much useful information as possible to help parents keep their children safe online outside of the school. This information is open to carers and extended family such as grandparents as well.

This is achieved via

- letters, newsletters, web site.
- parents evenings
- workshops

All members of staff are happy to provide support to parents but they are obliged to refer any contact if they suspect that there may be e-safety concerns.

5. Education and training for staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- a planned programme of formal e-safety training will be made available to staff
- an audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process
- this E-Safety policy and its updates will be presented to and discussed by staff prior to adoption, and as part of on-going review
- the school will seek to provide the best advice on practice to support E-Safety training as required to individuals and groups

6. E-Security

The School will take all reasonable steps to maintain a safe and secure environment. To this end:

- school ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined by the Aletheia Anglican Academies Trust.
- there will be regular reviews and audits of the safety and security of school ICT systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- all users will have clearly defined access rights to school ICT systems
- all users will sign an appropriate 'Acceptable Use Policy' before using the Internet
- the master/administrator passwords for the school ICT system used by the Network Manager must also be available to the Headteacher or other nominated senior leader and kept in a secure place
- in the event of technical support (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher
- any filtering issues should be reported immediately to the Aletheia Anglican Academies Trust.
- requests from staff for sites to be removed from the filtered list will be considered by the Aletheia Anglican Academies Trust via their support mechanism for doing so
- school /Trust ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy
- any actual/potential e-safety incident should be reported to the relevant person(s) which in most cases will include the e-safety co-ordinator, unless there are concerns about their conduct, in which case it should be escalated to involve SMT or the Headteacher
- staff must only use approved, encrypted memory sticks to store/transfer information
- the school infrastructure and individual workstations are protected by up to date virus software
- personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured

The use of digital imaging technologies has significant benefits to learning, allowing staff and children instant use of images that they have recorded themselves or downloaded from the internet. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet. Such images may remain available on the internet forever as part of a digital footprint, and may cause harm or embarrassment to individuals in the short or

longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees.

Staff should be aware of, and understand, the school's policy on staff use of social networks as outlined:

- when using digital images, staff should inform and educate children about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- staff are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes
- care should be taken when taking digital/video images that children are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute
- children must not take, use, share, publish or distribute images taken in school, of others, without permission of the subject and the school
- photographs published on the website, or elsewhere that include children, will be selected carefully and will comply with good practice guidance on the use of such images
- children's full names will not be used anywhere on a website or blog, particularly in association with photographs
- written permission from parents or carers will be obtained before photographs of children are published on the school website

7. Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate
- kept no longer than is necessary
- processed in accordance with the data subject's rights
- secure
- only transferred to others with adequate protection.

Staff must ensure that they take care at all times to ensure the safe keeping of any critical data, minimising the risk of its loss or misuse. They must store personal or critical data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.

8. E-Communication

The School provides all staff with an e-mail account for use in connection with their duties. It is expected that users of the system recognise that they are representing the school in any correspondence they undertake via this system and therefore have a duty to act with due care and regard to their actions.

Users of the system should be aware of the following:

- the school e-mail system may be regarded as safe and secure. It is virus checked and monitored, and should be used in all school related communications
- personal e-mail accounts should be used for private communications
- personal e-mail accounts should not be accessed on the school systems unless permission is given to do so outside of teaching times
- e-mail and internet communications may be monitored
- all users must immediately report to the nominated person(in accordance with the school policy) the receipt of any e-mail that makes them feel uncomfortable, is offensive, threatening or bullying in nature - users must not respond to any such email
- any digital communication between staff and pupils or parents / carers (e-mail etc.) must be professional in tone and content. These communications may only take place on official (monitored) school systems
- personal e-mail addresses, text messaging or public chat / social networking programmes must not be used for these communications
- children will be taught about good e-mail practices, safety issues, and how to respond to the risks attached to the use of e-mail

9. Illegal and unacceptable internet activity

The school believes that the activities below would be illegal, and/or unacceptable in a school context and that users of the school systems should not engage in these activities. The school policies and systems restrict and forbid certain Internet usage. Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- child sexual abuse images
- promotion or conduct of illegal acts e.g. under safeguarding/child protection, obscenity, computer misuse and fraud legislation
- adult material that potentially breaches the Obscene Publications Act in the UK
- criminally racist material in UK
- pornography
- promotion of any kind of discrimination
- promotion of racial or religious hatred
- threatening behaviours, including promotion of physical violence or mental harm
- any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute
- using school systems to run a private business
- use of systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Aletheia Anglican Academies Trust and / or the school

- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information e.g. financial / personal information, databases, computer / network access codes and passwords
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic e.g. downloading / uploading files that causes network congestion and hinders others in their use of the internet
- online gaming (educational and/or non-educational)
- online gambling
- online shopping / commerce
- use of social networking sites
- publishing to YouTube or similar sites

10. Responding to incidents of misuse

It is hoped that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

All concerns regarding E-Safety either with regard to children safety or user misconduct should be reported to the designated person for child safety and or the Headteacher and the schedule for reporting incidents followed accordingly as for any aspect of child safety or welfare or staff misconduct.