All Saints' Church of England Primary School

E-Safety Policy

Presented to and adopted by staff: **Sept 2017**

Presented to and adopted by governors:

Future Review Date: **Sept 2018**

Signed _____

Overview

This school has made significant investment in information technology and computer systems to support teaching and learning and to give learners the opportunity to seek information and carry out research. Access to the internet carries with it the danger that learners could find and view material that is unsuitable for them or that they could be put at risk from cyber bullying, unwanted and inappropriate contacts. This policy seeks to ensure that the internet and other forms of information communications technology are used appropriately for learning but with safeguards to protect learners from harm.

Objectives

• Managing on-line technology so that children are kept as safe as possible.
• The responses necessary when a risk to a child is discovered.

Safeguarding children, including e-safety is everyone's responsibility; e-safety is therefore not just the responsibility of the ICT coordinator/Headteacher, it is a whole school approach.

The overall aims of this policy are to ensure that children:

• Are equipped to access risks in a digital environment
• Are enabled to make informed judgments about such risk
• Know what to do if something 'not quite right' happens (e.g. they are exposed to inappropriate content or undesirable contact)

Strategies

Teaching and Learning

E-safety is taught throughout the school and integrated into all aspects of the Computing Curriculum. Each year group follow an e-safety road map linked to the computing scheme of work and are taught discreet e-safety skills in addition to this through events such as Safer Internet Day.

We use the 5 SMART targets

The 'Five **SMART** E-Safety Areas' are as follows:

S – Safe – This gives the children an overview of how to keep safe on the internet, from what information to share online to who you are speaking to. As well as this the children are advised when and where to use personal devices, such as mobile phones and IPADS.

M – Meeting – This makes the children aware that meeting someone online is extremely dangerous and that it should not be done under any circumstances. 'Online Friends Stay Online!'

A – Accepting - This focuses on potential problems that can arise from opening unknown files, E-Mails, Texts, etc.

R – Reliable – This shows the children how easy it is to be misled either on the internet or over the phone, via text. As well as this the children are made aware of the fact that not all the information they find and read online is always true.

T – Tell – This highlights that it is vital to tell somebody, like a friend, teacher, parent if they have got any issues. We also cover Cyber-Bulling and its effects.

Research indicates that children who are given greater freedom at school to use new technologies have a better knowledge and understanding of how to stay safe online. It is therefore important that the school runs a 'managed system' that helps children to become safe and responsible users of technology by allowing them to take more responsibility and manage their own risk. We believe that children become more vulnerable if they are not given the opportunity to learn how to assess and deal with online risk for themselves.

Why we use on-line technology?

The purpose of using on-line technology in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and business administration systems. Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

How does on-line technology enhance learning?

The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils. Children are taught what on-line technology use is acceptable and what is not and given clear objectives for its use. Children are educated in the effective use of on-line technology in research, including the skills of knowledge location, evaluation and retrieval.

Managing the Use of On-line Technology

Acceptable Use Policy (AUP)

This sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of on-line technologies. The AUP details how we provide support and guidance to parents / carers for the safe and responsible use of these technologies by adults and children. Each user signs a contract to ensure that they know what is deemed 'acceptable use of the Internet'.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone.

• Staff are provided with an individual email log-in username.
• Staff are instructed to inform the ICT coordinator if they think their password has been compromised or someone else has become aware of their password.
• Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks ensuring that passwords are not shared and are changed periodically.

• Staff should ensure that computers and lap tops are password protected and not left unattended.
• All work, data and images stored on portable devises must be password protected or encrypted.

Internet Access

The school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of the pupils. Internet access is planned to enrich and extend learning activities. Parents of all pupils are asked to sign and return a consent form giving permission for their child to use the Internet.

• In Foundation Stage and Key Stage 1, access to the Internet is by adult demonstration and direct supervised access to specific, approved on-line materials.
• In Key Stage 2, pupils will work independently using the internet, but will not be left unsupervised. Pupils are taught the importance of e-safety and agree terms and conditions for acceptable Internet use. Pupils are taught to be critically aware of the materials they read and are made aware that information may be not always be reliable or accurate.

The school website:

• The point of contact on the website should be the school address, school e-mail and telephone number. Staff or pupils' home information will not be published.
• Web site photographs that include pupils will be selected carefully.
• Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
• Permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Chat and instant messaging

• Pupils will not be allowed access to public or unregulated chat rooms.
• Pupils will not access social networking sites for example 'My Space', 'Facebook', 'Twitter', 'Instagram 'etc
• Any form of bullying or harassment is strictly forbidden.

Filtering

• The School works in partnership with parents, Remedian and DFE to ensure that systems are in place to protect pupils.
• If staff or children discover unsuitable sites, the URL (address) and content must be reported to Remedian via the ICT coordinator or the office staff.
• Any material that the school believes to be illegal must be referred to the Internet Watch Foundation (IWF).

Photographic, video and audio technology

• Care should be taken when capturing photographs or video to ensure that all pupils are appropriately dressed.

• Staff may use photographic or video devices to support school trips and curriculum activities. School equipment should be used for this purpose. Should personal equipment ever be used, then all images must be transferred to school hardware and deleted from the personal device as a matter of urgency.
• Audio or video files may only be downloaded if they relate directly to the current educational task being undertaken.
• Pupils should always seek the permission of their teacher before making audio or video recordings within school grounds.

Mobile Phones (see Mobile Phone Policy)
• Children are not encouraged to bring mobile phones in school and are not allowed to use them in school.
• Staff must have their mobile phones on 'silent' during teaching times.
• The sending of abusive or inappropriate text messages is strictly forbidden.

Emerging ICT Applications
• Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Complaints Regarding the Use of On-line Technology
Prompt action is required if a complaint is made. The facts of the case must be established and presented to the ICT coordinator (who will inform the Headteacher/member of the SLT). A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could be potentially more serious and a range of sanctions will be used, linked to the School's Behaviour Policy. Complaints of a child protection nature will be dealt with in accordance with Rochdale LEA child protection procedures and our school policy.

Any complaints about staff misuse of on-line technology must be referred directly to the head teacher.

How to Respond When a Risk is Discovered
The ICT coordinator will ensure that the following procedures are adhered to in the event of any misuse of the internet:

An inappropriate website is accessed inadvertently:
• Report website to the e-safety lead.
• Contact Remedian so that the site can be added to the banned or restricted list.
• Change Local Control filters to restrict locally.
• Log the incident.

An inappropriate website is accessed deliberately:
• Ensure that no one else can access the material by shutting down the computer.
• Log the incident.
• Report to the head and ICT coordinator immediately.
• Head to refer back to the Acceptable Use Rules and follow agreed actions for discipline.
• Inform the filtering services in order to reassess the filters.

An inappropriate website is accessed deliberately by a child:

• Refer the child to the Acceptable use Rules that were agreed.
• Reinforce the knowledge that it is illegal to access certain images and police can be informed.
• Log the incident
• Decide on appropriate sanction.
• Notify the parent / carer.
• Contact the filtering service (Remedian) to notify them of the website.

An adult receives inappropriate material:

• Do not forward this material to anyone else – doing so could be an illegal activity.
• Alert the ICT coordinator and head teacher immediately.
• Ensure the device is removed and log the nature of the material.
• Contact relevant authorities for further advice e.g. police, social care, CEOP (Rochdale Sunrise Team).
• Log the incident.

An illegal website is accessed or illegal material is found on a computer.

The following incidents must be reported directly to the police:

• Indecent images of children found. (Images of children whether they are photographs or cartoons of children or young people apparently under the age of 16, involved in sexual activity or posed in a sexually provocative manner)
• Incidents of 'grooming' behaviour.
• The sending of obscene materials to a child.
• Criminally racist or anti-religious material
• Software piracy
• The promotion of illegal drug-taking
• Adult material that potentially breaches the obscene publications act in the UK.

If any of these are found, the following should occur:

• Alert the Headteacher/ ICT coordinator immediately.
• DO NOT LOG OFF the computer but disconnect from the electricity supply.
• Contact the police and or CEOP (Rochdale Sunrise Team) and social care immediately
• If a member of staff or volunteer is involved, refer to the allegations against staff policy and report to the Local Authority Designated Officer.

An adult has communicated with a child or used ICT equipment inappropriately (e-mail/text message etc)

• Ensure the child is reassured and remove them from the situation.
• Report to Headteacher and Designated Person for Child Protection immediately, who will then follow the Allegations Procedure and Child Protection Procedures
• Report to the Local Authority Designated Officer.
• Preserve the information received by the child if possible.
• Contact the police as necessary.

Threatening or malicious comments are posted to the school website or facebook page (or printed out) about an adult in school:

• Preserve any evidence and log the incident.
• Inform the Headteacher immediately who will then take any appropriate actions felt necessary.
• Inform the ICT coordinator that new risks can be identified.
• Contact the police or CEOP (Rochdale Sunrise Team) if appropriate.

Where staff or adults are posted on inappropriate websites or have inappropriate information about them posted this should be reported to head teacher and ICT coordinator.

Threatening or malicious comments are posted to the school website or facebook page about a child in school or malicious text messages are sent to another child/young person (cyber bullying)

• Preserve any evidence and log the incident.
• Inform the ICT coordinator immediately and the Headteacher who will follow the Child Protection Policy.
• Check the filter if an internet based website issue.
• Contact/parents and carers
• Refer to the bullying policy
• Contact the police or CEOP (Rochdale Sunrise Team) as necessary.

Outcomes

That all staff are aware that safeguarding children, including e-safety is everyone's responsibility; e-safety is therefore not just the responsibility of the ICT coordinator, it is a whole school approach. Staff can manage on-line technology so that children are kept as safe as possible. As a school we respond where necessary when a risk to a child is discovered. Children are equipped to access risks in a digital environment and are able to make informed judgments about such risk. Children know what to do if something 'not quite right' happens (e.g. they are exposed to inappropriate content or undesirable contact)