Abbots Ripton Church of England Primary School

E-Safety Policy

Written by: Claire Matthews (based on a model policy from Cambridgeshire ICT Service February 2019)

Date: September 2019

Review date: September 2021

Our church school creates a firm foundation where together, with God's help and with the help of others, we learn for life, achieve our best and grow in faith.

Contents

Background to this policy:

The purpose of this policy is to describe the safeguarding measures in place for adults and children in school in relation to online safety, including:

- The policies and practice embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age appropriate online safety curriculum for all pupils

Online safety in schools is primarily a safeguarding concern and not a computing / technology one. Therefore this policy should be viewed alongside other Safeguarding policies and approaches including, but not limited to:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Safeguarding and Child Protection
- Personal Social Health Citizenship Education (PSHCE)
- Safer Working Practices
- Data Protection Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Cambridgeshire Progression in Computing Capability Materials
- Whistle Blowing Policy

This policy must be read alongside the staff and pupil Acceptable Use Policies attached as appendices. These AUPs outline the expectations and sanctions which apply to staff and pupil use of technology.

- The development of our E-Safety policy involved:
    - The Headteacher
    - The Designated Safeguarding Lead
    - Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
    - The governor responsible for Safeguarding

- This policy may also be partly reviewed and / or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email is readily available on the school staff share. It has also been made available to parents via the school website.

- All staff must be familiar with this policy and all staff and pupils must sign the relevant Acceptable Use Policy before being allowed to access school's systems (see appendices). As Online safety is an important part of strategic leadership within the school, all staff have a shared responsibility to ensure that the policy and practices are embedded. This will be monitored by the Headteacher, the Designated Safeguarding Lead and governors as appropriate.

Rationale:

- At Abbots Ripton CofE Primary School we believe that the use of technology in schools brings great benefits. To live, learn and work successfully in an increasingly complex and information-rich society, our children must be able to use technology effectively.

The use of these exciting and innovative technology tools in school and at home has been shown to support learning and promote pupil achievement. Yet at the same time, we recognise that the use of these new technologies can put young people at risk within and outside the school.

The risks they may face can broadly be categorised into the '3 C's' **Contact**, **Content** and **Conduct** (Livingston and Haddon) and may include:

- Access to harmful, illegal or otherwise unsuitable content including gaming, gambling sites, sexually explicit material and websites with extremist ideologies and images
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet, including the sharing of Self-Generated Indecent Images
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Cyber-bullying
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading or streaming of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

While children and young people need support to keep them safe online, the risks associated with the use of technology are not restricted to just them. Online safety issues can also affect adults who work or are associated with the school and this will be referenced in more detail later in this policy.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops, iPads and also desktops in the office including staff level internet access, server access and access to MIS systems.
- Staff have access to school systems beyond the school building (e.g. MIS systems and cloud storage of school files). Staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards.

Pupils:

- Pupil laptops and iPads including filtered access to the Internet and pupil level access to areas of the school network.
- Cameras and peripherals including programming resources (Beebots, control equipment etc.)

Where the school changes the use of existing technology or introduces new technologies which may pose risks to pupils' safety, a risk assessment will be completed to show how the risk is being mitigated and reduced to an acceptable level.

Church of England's Digital Charter - 1st July 2019

The Church of England has produced a Digital Charter, designed for use by anyone engaging with its online accounts and we echo the messages in this charter to support our online safety.

The charter includes:

•Be safe. The safety of children, young people and vulnerable adults must be maintained.

•Be respectful. Do not post or share content that is sexually explicit, inflammatory, hateful, abusive, threatening or otherwise disrespectful.

•Be kind. Treat others how you would wish to be treated and assume the best in people. If you have a criticism or critique to make, consider not just whether you would say it in person, but the tone you would use.

•Be honest. Don't mislead people about who you are.

•Take responsibility. You are accountable for the things you do, say and write. Text and images shared can be public and permanent, even with privacy settings in place. If you're not sure, don't post it.

•Be a good ambassador. Personal and professional life can easily become blurred online so think before you post.

•Disagree well. Some conversations can be places of robust disagreement and it's important we apply our values in the way we express them.

•Credit others. Acknowledge the work of others. Respect copyright and always credit where it is due. Be careful not to release sensitive or confidential information and always question the source of any content you are considering amplifying.

•Follow the rules. Abide by the terms and conditions of the various social media platforms themselves. If you see a comment that you believe breaks their policies, then please report it to the respective company.

The online safety curriculum:

When using online technologies, it is essential that children understand how to behave in a safe and responsible manner and also how to react when faced with inappropriate content or situations which make them feel uncomfortable. The need for a progressive, age appropriate online safety curriculum is clearly documented in the National Curriculum for Computing which states that:

- **At KS1:** use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
- **At KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Abbots Ripton CofE Primary School we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. We believe that just as children learn how to swim by going to a swimming pool so they will learn safe life-long online behaviours by accessing and using a range of online services including the World Wide Web.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials and is linked to demonstrating safe practice in our online learning platform, (Starz+).
- Our programme for online safety education is evidenced in teachers' planning both as discrete, embedded and continuous activities.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching and communicating in appropriate online environments.

Continued Professional Development:

- Staff at Abbots Ripton CofE Primary School receive up-to-date information and training on online safety issues in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.
- Nominated members of staff receive more in-depth online safety training to support them in keeping up to date and reviewing the school's approach, policies and practice.
- New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online.

- All staff have been made aware of individual responsibilities relating to the safeguarding of children within the context of online safety and know what to do in the event of misuse of technology by any member of the school community.

School website:

Schools are required to publish certain information online – which in practice means we must have a school website.

The main purpose of our school website is to provide information. Our school website will not only tell the world that our school exists, but it will provide information for our pupils and parents, promote the school to prospective ones and publish as a minimum the statutory information required by the Department for Education.

In conjunction with a range of online services, our school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

Under safeguarding responsibilities, it is our duty to ensure that every child in our care is safe, and the same principles apply to the virtual presence of a school as it would apply to its physical surroundings. We therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, information displayed on the school website.

The school has established a Website Strategy to ensure that our website is maintained, is effective, and does not compromise the safety of the pupils or staff.

Mobile devices and use of 3G and 4G data in school:

We do not allow pupils to bring their own devices into school and this includes mobile phones, iPads and SMART watches. If there is a need for them to do so, we ask that parents inform us and the device will be switched off and kept by the school office during the school day. It will then be returned to the pupil at the end of the day.

Monitoring, and averting online safety incidents:

The school keeps children safe when using online technologies through a combination of online safety education, filtering and monitoring children's online activity and reporting incidents, including following Safeguarding procedures where appropriate.

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both the East of England Broadband Network (E2BN) and the Local Authority's Education ICT Service. Safeguards built into the school's infrastructure include:

- Secure, private CPSN provided internet connection to each school with a direct link to the National Education Network.
- Managed firewalling running Unified threat management (UTM) that provides Restrictions on download of software, apps and file types from known compromised sites.
- Base line and optional enhanced filtering.
- Optional SSL decryption available on web traffic to allow for greater visibility of sites being accessed and requested.
- Antivirus package provided as part of CPSN Connection.
- Email system for all school staff with direct internal routes to the council for trusted email communications.
- Wireless networks installed by The ICT Service are encrypted to industry best practice standards and the wireless key should be kept securely by the school office.

Staff also monitor pupils' use of technology and, specifically, their activity online.

Pupils' use of online services (including the World Wide Web) are supervised in school at all times.

Staff are also able to monitor pupils' activity on our online learning platform (Starz+), allowing them to identify inappropriate or concerning online behaviour, as well as respond to reports of any such behaviour from pupils or parents.

A system of staff and pupil passwords is in place to enable appropriate access to the school network.

- All members of staff have individual, password protected logins to the school network and MIS systems.
- Visitors to the school such as supply teachers can access part of the school systems using a generic visitor login and password.
- The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the school office.
- School staff, Governors and visitors for whom access is essential as part of their role, are able to connect personal devices to the school's wireless network with the permission of the Headteacher or Deputies on a case by case basis.

Whilst we recognise that it is impossible to totally eliminate the risks associated with the use of technology, these safeguards are in place to help minimise these risks as much as possible.

Responding to online safety incidents:

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an online safety incident occurs or they suspect a child is at risk through their use of technology.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. This may mean that serious actions have to be taken in some circumstances.
- If an online safety incident occurs, staff complete an E-safety Incident log in line with our safeguarding logging procedures. The actions as a result of this may include internal sanctions and involvement of parents.

In addition, the Education and Inspections Act 2006 empowers headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents which may take place outside of the school but has an impact within the school community.

- With this in mind, the headteacher may decide to apply the sanctions and / or procedures in the relevant AUP to incidents which occur outside of schools if s/he deems it appropriate.

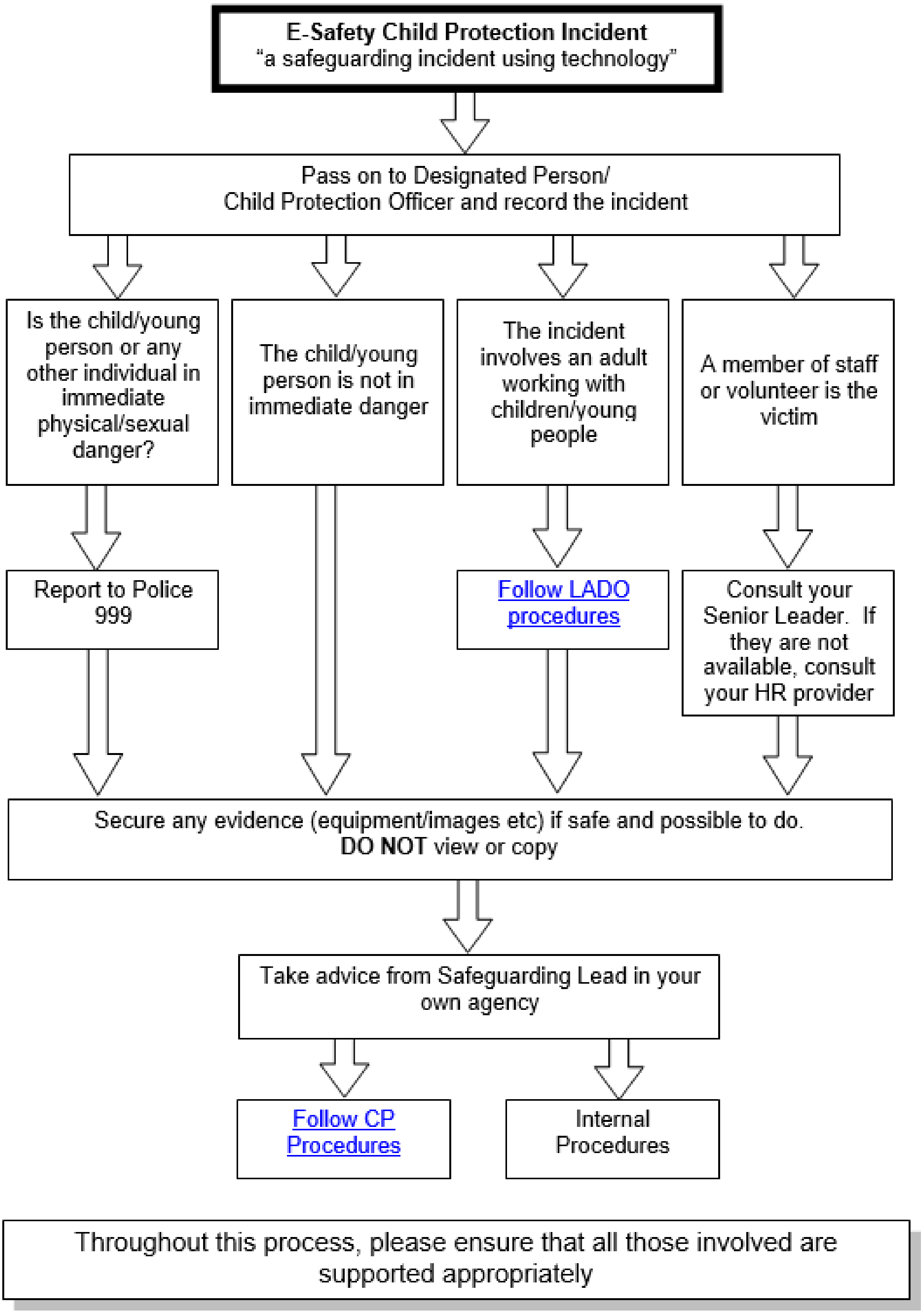
The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.

In our school, the likelihood of these types of instances occurring are already reduced as we don't allow pupils to use personal devices in school.

Where the school suspects that an incident may constitute a Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.

You come across a child protection concern involving technology …



E-Safety Child Protection Incident
"a safeguarding incident using technology"

Pass on to Designated Person/
Child Protection Officer and record the incident

Is the child/young person or any other individual in immediate physical/sexual danger?

The child/young person is not in immediate danger

The incident involves an adult working with children/young people

A member of staff or volunteer is the victim

Report to Police 999

Follow LADO procedures

Consult your Senior Leader. If they are not available, consult your HR provider

Secure any evidence (equipment/images etc) if safe and possible to do.
DO NOT view or copy

Take advice from Safeguarding Lead in your own agency

Follow CP Procedures

Internal Procedures

Throughout this process, please ensure that all those involved are supported appropriately

Appendix A

Staff E-Safety
Acceptable Use Policy

This policy covers the following aspects of e-safety in relation to all school staff:

- Use of school based equipment
- Social Networking
- Managing digital content
- Email
- Mobile phones and devices
- Learning and teaching

All staff should read and sign this document to demonstrate that they agree with the statements.

Use of school based equipment

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

- 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 Head teacher.
- I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords.
- I will seek consent from the Headteacher prior to the use of any new technologies (hardware, software, cloud-based services) 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 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 office manager.
- 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.
- No personal data will be stored on any portable storage (USB sticks, SSD cards, portable hard drives etc).
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned laptop 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 from the Head teacher.
- 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.

Social Networking

- 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 Head teacher. If requested I will complete an E-safety log of concern.

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 permissions form completed by parents.
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from the 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 licencing.
- 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 ensure that any images taken on school-owned devices will be transferred to the school network (server) and deleted as soon as possible from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. 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.

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 seek permission if I need to synchronise any school email account with a personally-owned handheld device.
- 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 if necessary authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, 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.
- Emails which refer to pupils at the school will just use initials and documents sent as attachments which contain lots of pupil data will be password protected and the password shared face to face or by telephone.

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 the Head teacher.
- If I need to contact any parents on my personally-owned device I will ensure that my caller identification is switched off.
- I will not use any personally-owned mobile device to take images, video or sound recordings.
- I understand that the school has a separate Mobile Phone Policy which I will also read.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach an age appropriate e-safety curriculum.
- I will support and promote the school e-safety 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 e-safety 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.

Agreement

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 understand that if I fail to comply with this Acceptable Use Policy agreement, I could be subject to disciplinary action.

Name :
Role in School:
Signed
Date:

Appendix B

Acceptable Use Agreement – EYFS/KS1 Pupils

THINK BEFORE YOU CLICK	
S	Surfing: I will only use the Internet with adult supervision
A	Access: I will only click on icons and links when I know they are safe
F	Friendly: I will only send friendly and polite messages
E	Eeek!: If I see something I don’t like on a screen, I will always tell an adult

My Name:	
My Signature: **(or Parent/Guardian’s Signature)**	
Parent/Carer’s Name:	

Appendix C

Acceptable Use Agreement – KS2 Pupils

I will

- Use school ICT equipment for schoolwork and homework.
- Only use the internet and email when an adult is nearby.
- Keep my password ‘Top Secret’.
- Tell my teacher if I think someone else knows my password.
- Only use my Starz e-mail address when e-mailing.
- Ask an adult before opening an email from someone I don’t know.
- Send friendly and polite messages.
- Ask my teacher before using photos or video.
- Report anything I think is mean or offensive to an adult.

I will not

- Share my username and password.
- Share details about myself such as surname, phone number or home address.
- Send or display offensive messages or pictures.
- Use bad language.
- Trespass in others' folders, work or files.
- Intentionally waste resources.
- Plug anything into school equipment without permission.

Sanctions

Abuse of the above rules will result in a temporary or permanent ban on Internet use.
When applicable parents may be involved.

………

I have read the above rules. I understand what I have read. I agree to follow these rules when:

- I use the school ICT equipment.
- I am allowed to use my own equipment in school.
- I use my own equipment out of school in a way that is connected to me being a member of this school eg. using Starz to communicate and collaborate with other members of the school community.

Name:	**Signed:**
Class:	**Date:**