

Robert Arkenstall Primary School

Online Safety Policy

(also referred to in this document as e-safety policy)

It is the aim of Robert Arkenstall Primary School to provide a broad curriculum and education of the highest quality within a happy, safe, secure and stimulating environment, which enables each child to experience success; to equip them with skills as thoughtful, caring and active citizens, eager to explore the possibilities of the world.

pursue possibilities; love learning

This policy is published on the School website, stored on the Network: Staff Share and is available on request from the school office

Governor Committee	Finance & Personnel
Reviewer	D Hodge
Ratified	October 2021
Review period	1 year
Next review due	October 2022

Contents

- **Background to the policy**
- **Rationale**
- **The e-safety curriculum**
- **Continued professional development**
- **Safeguarding Children online**
- **Responding to e-safety incidents**
- **Glossary**
- **Appendices (including Acceptable Use agreements)**

Background to the policy

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

- **The policies and practices we have developed in school for using the Internet and online technologies**
- **How these fit into the wider context of our other school policies**
- **The methods used to protect children from sites containing pornography, racist or politically extreme views and violence.**

Ultimately, the responsibility for setting and conveying the standards that children are expected to follow when using technology, media and information resources, is one the school shares with parents and carers. At Robert Arkenstall Primary School, we feel that the most successful approach lies in a combination of site filtering, of supervision and by fostering a responsible attitude in our pupils in partnership with parents.

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

- Behaviour Policy
- Safeguarding and Child Protection Policy
- Acceptable Use Policy and agreements- staff, pupil, parents
- Social Media Policy
- Mobile Phone and Devices Policy
- RSE Policy (Relationships and Sex Education)
- Citizenship and PSHE Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Computing and ICT Policy

Related guidance documents include:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Guidance on Safer Working Practice for Adults who work with children and Young People
- County guidance (e.g. Use of Digital Images, e-mail)
- LA Infrastructure guidance (E2BN)
- Cambridgeshire Progression in ICT Capability Materials
- Risk assessment log
- Incident Log

This policy may also be partly reviewed and / or adapted in response to specific e-safety incidents or developments in the school's use of technology. It has been shared with all staff via email and a staff meeting and is readily available on the school network and 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 E-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 Person for Child Protection and governors.

Rationale

At Robert Arkenstall Primary school we believe that the use of information and communication technologies 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 raise educational standards 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
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others
- Online Bullying (known sometimes as Cyber-bullying), including comments left on online platforms such as blogger/vlogs.
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading 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
- The danger of children willingly giving away personal information online which could provide problems for them
- The risk of being radicalized through accessing terrorist and extremist material

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 are school representatives. For example, school and personal data being entered on web/social networking sites, fraudulent email traps and cyberbullying. It is impossible to eliminate risk completely. It is therefore essential, through good educational provision to manage the risk and deal with any threat to safety.

Technologies regularly used by pupils and staff include:

Staff:

- Staff laptops including staff level internet access, server access and access to MIS systems
- Staff laptops can also be used at home in accordance with the staff AUP and GDPR
- Cameras and video cameras, visualisers (see Mobile Phones and Devices Policy)
- Curriculum iPads for preparing and delivering pupil activities
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards

Pupils:

- Curriculum iPads and school laptops 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, class cameras etc.)

Others on school premises:

- Limited access to school systems such as filtered internet access using a visitor login.

The school's ICT 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.

E2BN's Protex web filtering system received full Becta (British Educational Communications and Technology Agency) accreditation in 2007 by blocking over 90% of all inappropriate material. E2BN also manage a distributed caching service which is integrated with the web filtering service.

Ref: E2BN Website

This helps to ensure that staff and pupils rarely encounter material which is inappropriate or offensive. If / when they do, the school's AUPs and online-safety education programme ensure that they are equipped to deal with any issues in the most appropriate way.

Whilst we recognise the benefits of individual pupil logins to our school network, all teachers can use a year group login for ease of access – which is particularly common in KS1. As pupils move into KS2 they will increasingly use individual logins.

All members of staff have individual, password protected logins to the school network. Relevant volunteers, such as librarians, have individual, password protected logins with restricted access to the school network and visitors to the school can access part of the network using a generic visitor login and password.

The school's network can either be accessed using a wired or wireless connection. However, the wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by nominated staff within the school. School staff and pupils are not permitted to connect personal devices to the school's wireless network and the wireless key is only given to authorised visitors on official school business if felt necessary to complete their official school related business.

Where visitors under the age of 18 may need limited access to the school network (such as secondary school work experience visitors), they are considered as pupils and login using a designated pupil visitor login with restrictions on internet access and network access the same as those given to Robert Arkenstall pupils.

The e-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 e-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 Robert Arkenstall Primary School we believe that a comprehensive programme of e-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.

We have planned a range of age-related teaching and learning opportunities to help our pupils to become safe and responsible users of new technologies. These opportunities include:

- Discrete and embedded activities drawn from a selection of appropriate materials (such as ThinkUKnow and Google's Be Internet Legends).
- Posters and reminders in and around the school.
- Key e-safety messages that are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in discussion forums.
- Related work in PSHE lessons, including statutory elements of RSE and Health Education.

Continued Professional Development:

- Staff at Robert Arkenstall Primary School receive up-to-date information and training on e-Safety issues in the form of staff meetings and updates from Computing Subject Leader, as well as training from external providers where appropriate.
- 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 e-Safety and know what to do in the event of misuse of technology by any member of the school community.

Safeguarding Children Online

Our School recognises that different users will be expected to use the school's technology systems in different ways – appropriate to their age or role in school. We acknowledge the need to:

Equip children to deal with exposure to harmful and inappropriate content and contact, and equip parents to help their children deal with these things and parent effectively around incidences of harmful and inappropriate conduct by their children.

UKCCIS (The UK Council for Child Internet Safety) – June 2008

The school has published an Acceptable Use Policy and agreements for pupils and staff who sign to indicate their acceptance of our AUPs and relevant sanctions which will be applied should rules be broken. Please see appendices for full details.

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 our pupils and parents, promote the school to prospective parents and pupils, and publish the statutory information required by the Department for Education.

In conjunction with a range of online services, a 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. As a school, we ensure that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website.

Responding to E-safety Incidents

It is important that all members of staff – teaching and non-teaching – are aware of how to respond if an e-safety incident occurs or they suspect a child is at risk through their use of technology. It is important that responses to e-safety incidents are 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 Robert Arkenstall Primary School will follow its agreed procedures for dealing with incidents including internal sanctions and involvement of parents (this may include the deactivation of accounts or restricted access to systems as per the school's AUPs – see appendix).

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 e-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.

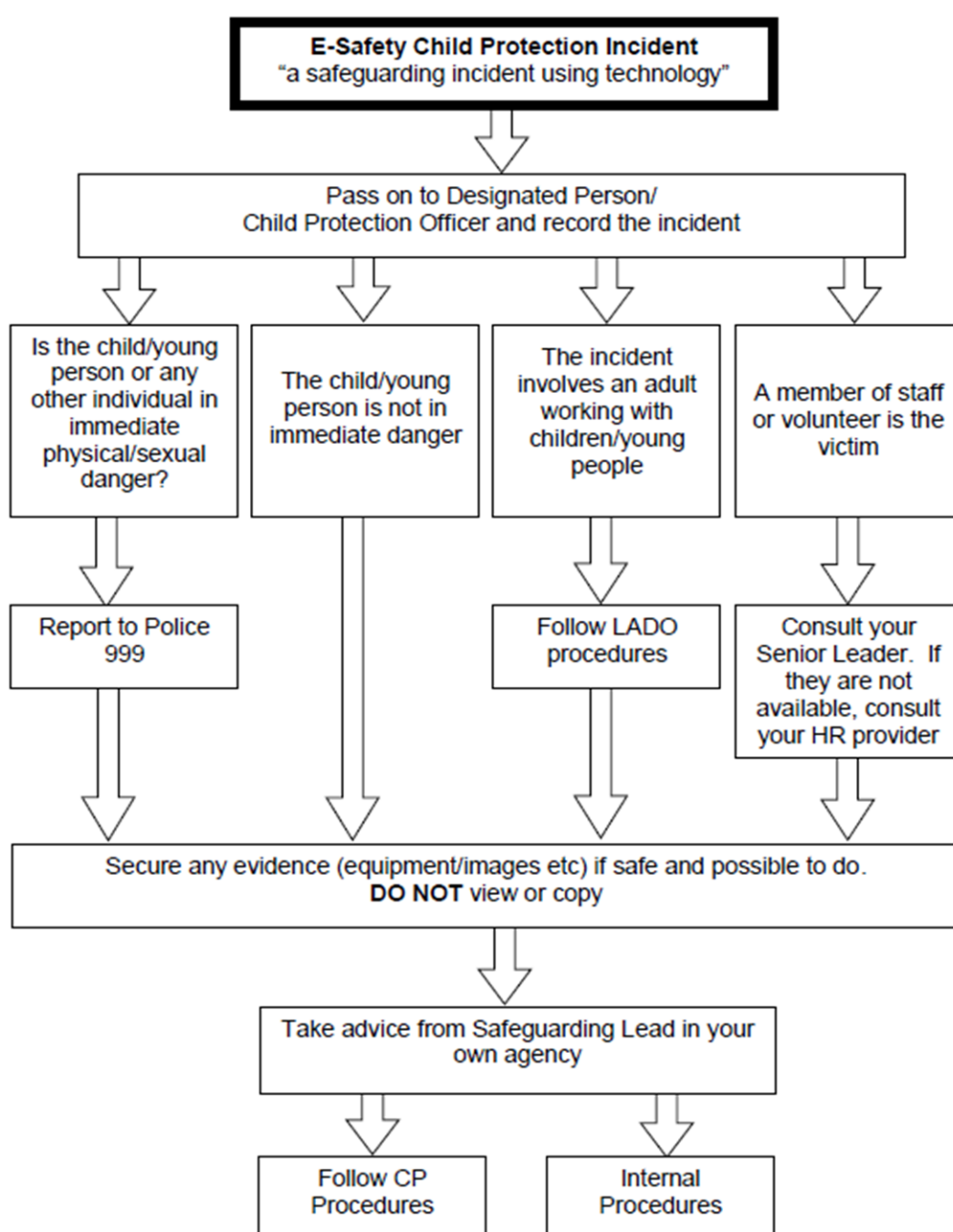
The Education Act 2011 gives school staff the powers, in some circumstances to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

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 with parents (where appropriate) before taking any further action.

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

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

You come across a child protection concern involving technology ...



Dealing with Incidents and Seeking Help

If a concern is raised, refer immediately to the designated person for child protection. If that is not possible refer to the headteacher or, if necessary, the Chair of Governors.

It is **their** responsibility to:

Step 1: Identify who is involved – any combination of child victim, child instigator, staff victim, or staff instigator

Step 2: Establish the kind of activity involved and whether it is illegal or inappropriate. If in doubt they should consult the Education Child Protection Service helpline.

Step 3: Ensure that the incident is documented using the standard child protection incident logging form (see appendix)

Depending on the judgements made at steps 1 and 2 the following actions should be taken:

Staff instigator – follow the standard procedures for Managing Allegations against a member of staff. If unsure seek advice from the Local Authority Designated Officer or Education Officer.

Staff victim – Seek advice from your Human Resources (HR) provider and/or Educational Child Protection Service

Illegal activity involving a child – refer directly to Cambridgeshire Constabulary – 0845 456 4564 – make clear that it is a child protection issue

Inappropriate activity involving a child – follow standard child protection procedures. If unsure seek advice from Education Child Protection Service helpline.

Equally, if the incident involves or leads to an allegation against a member of staff, the school will follow the agreed procedures for dealing with any allegation against a member of staff (see appendix).

Glossary

Terms used in this policy

AUA: Acceptable Use agreement: A document detailing the way in which new or emerging technologies may/may not be used – may also list sanctions for misuse. A signed agreement commits users to follow the guidance in this and related policies.

AUP: Acceptable Use policy

Child: Where we use the term ‘child’ (or its derivatives), we mean ‘child or young person’; that is anyone who has not yet reached their eighteenth birthday.

Online-safety: We use online-safety, and related terms such as ‘e-safety’, ‘communication technologies’, and ‘digital technologies’ to refer to all fixed and mobile technologies that children may encounter, now and in the future, which might pose e-safety risks. We try to avoid using the term ‘ICT’ when talking about e-safety as this implies that it is a technical issue – which is not the case. The primary focus of online-safety is child protection: the issues should never be passed solely to technical staff to address.

PIES: A model for limiting e-safety risks based on a combined approach to **P**olicies, **I**nfrastructure and **E**ducation, underpinned by **S**tandards and inspection. Whilst not explicitly mentioned in this policy, this model provides the basis for the school’s approach to online-safety.

Safeguarding: Safeguarding is defined (for the purposes of this document) as the process of increasing resilience to risks when using technology through a combined approach to policies and procedures, infrastructure and education, underpinned by standards and inspection. E-safety is just one aspect of a much wider safeguarding agenda within the UK, under the banner of Every Child Matters: Change for Children. Those with responsibility for the development and delivery of e-safety policies should embed their work within the wider safeguarding agenda, and work across services to ensure that they are delivering the best possible opportunities for the children and young people in their care.

Schools: For ease of reading we refer predominantly to schools within this publication, but the underlying principles can be applied equally to any setting with responsibility for educating or safeguarding children and young people.

Users: We use this term, and related terms such as service users and end users, to mean those people who will ultimately be bound by the provisions of an AUP. This might be pupils, staff, parents and carers, or members of the wider community, depending on provisions of your AUP or the context in which you operate.

Appendices

Appendix 1

Staff acceptable use Guidance and Agreement

To be read and adhered to by all adults working in school

(see AUP for definition)

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 never allow other users to access the internet through my username and password. I will lock my workstation when not in use. 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 e-safety coordinator.
- 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 e-safety coordinator/ 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 e-safety 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 / e-safety coordinator.
- 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 only use school-owned or provided portable storage (USB sticks, SSD cards, portable hard drives etc. without specific permission from a member of senior leadership team).
- 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 encrypted memory stick.
- I understand that school laptops, although password protected, are not encrypted and therefore no personal or sensitive information should be stored on them (all teachers have access to unlimited, secure online storage. See computing coordinator.)
- 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 network manager.

- 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 will abide by the guidelines set out in the school's Social Media Policy.

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 e-safety Policy/ Home School Agreement.
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- 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 (storage area/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.

Mobile phones and devices

- I will adhere to the content set out in the school's Mobile Phones and Devices policy.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach 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.

Appendix 2

Acceptable Use and Confidentiality Agreements

To be issued and signed by adults working in school at induction and after reviews

I accept and undertake to read and abide by the guidelines of the Acceptable Use Policy and agree to use the setting technology and my own devices within these guidelines.

I accept and undertake to read the Confidentiality Policy and agree to abide by the guidance related to this setting.

Appendix 3

AUA letter to parents

Dear Parent / Carer,

Re: Acceptable Use Agreement

As part of our computing and broader curriculum, we subscribe to a number of education web-based resources.

The web-based resources used by school provide children with a safe and secure online environment to explore the use of messaging, blogging, discussion groups and uploading work. Children may be given passwords to access them at home and at school, helping bridge the link between home-school learning. In addition to the taught computing curriculum, teachers will be using the facility to provide access to a range of learning resources across the curriculum.

Being a good e-citizen is an important part of learning in our school - teaching children to be safe and responsible online.

As part of our introduction to the technology, the children will be discussing and signing an acceptable use agreement for all digital technology in school.

I enclose a copy of this for your information.

As computing co-ordinator, Mr Hodge will oversee the use of school systems – ensuring the children are confident to use them appropriately.

Yours sincerely,

Kate Bonney
Head teacher

Appendix 4

Robert Arkenstall

Acceptable Use Agreement KS2

- **I will not send any messages that could be unkind or could upset anyone else. I'm aware that all information sent and received through educational school-based systems is recorded.**
- I will use the school's ICT equipment and tools (including computers, cameras, iPads etc.) for schoolwork and homework. If I need to use the school's computers for anything else, I will ask for permission first.
- I will only use the Internet with the permission of a teacher or teaching assistant and if they are in the room with me.
- I will only delete my own files unless my teacher gives me permission to delete someone else's. I will not look at other people's files without their permission.
- I will keep my passwords private and tell an adult if I think someone else knows them. I know that my teacher can change my school-based internet resource passwords if needed.
- I will only open e-mail attachments from people who I know or an adult has approved. If I am unsure about an attachment or e-mail, I will ask an adult for help.
- I will not give my own personal details such as surname, phone number or home address or any other personal details that could be used to identify me, my friends or my family. If I have to use an online name I will make one up!
- I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.

- I will not behave to others online in a way I know to be unkind, upsetting or annoying e.g 'trolling,' or 'hacking' (these examples are not exhaustive when using school-based resources either at home or at school).
- I will never arrange to meet someone I have only ever previously met online. It could be dangerous.
- I will not deliberately look for, save or send anything that could be unpleasant or upsetting. If I find anything via Internet, e-mail or mobile phone that is upsetting or makes me feel uncomfortable, I will tell a teacher or responsible adult.

I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, my teacher may:

- Speak to me about my behaviour.
- Speak to my parents about my use of technology.
- Remove me from school research internet resource communities or groups.
- Turn off my accounts for a little while or permanently.
- Not allow me to use laptops / computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.





Pupil's name:

Pupil's signature:

Date:

Appendix 5

Robert Arkenstall EYFS / KS1 Agreement Form

Think Before You Click!	
<p>S</p> 	<p>I will only use the Internet and email with an adult there.</p>
<p>A</p> 	<p>I will only click on icons and links when I know they are safe.</p>
<p>F</p> 	<p>I will only send friendly and polite messages.</p>
<p>E</p> 	<p>If I see something I don't like on a screen, I will always tell an adult.</p>
<p>Child's Name:</p> <p>I have discussed this with my child to explain what is expected of them and so they know what to do if there is an issue</p> <p>Signature:</p>	