

E-safety Policy and AUPs

Approved by the Governing Body in:

Autumn 2018

This revised policy includes a new AUP for staff following the introduction of GDPR and the new Keeping Children Safe in Education requirements.

Contents

- The background to this policy
- Rationale
- The e-safety curriculum
- Continued Professional Development
- Monitoring, and preventing e-safety incidents
- Responding to e-safety incidents
- Appendices (including AUPs)

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 e-safety, including:

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

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:

- Professional boundaries in relation to your personal internet use and social networking online – advice to staff (LSCB)
- Safeguarding and Child Protection
- Personal Social and Health Education (PSHE)
- 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 Officer for Child Protection
    - The Computing Subject Leader
    - Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service) and has been adapted from a template policy.
    - The governor responsible for Safeguarding

It was presented to the governing body's Finance and Resources committee and ratified on 22/11/2018 and will be formally reviewed in Autumn 2019.

- 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 Officers for Child Protection and governors.

Rationale:

- At Monkfield Park 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.
- 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 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. E-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.
- Some staff have access to MIS systems from home via a secure logon and sometimes additional authentication.
- Staff laptops can also be used at home in accordance with the staff AUP.

- Curriculum iPads for preparing and delivering pupil activities.
- Class cameras and other peripherals such as visualisers and Interactive Whiteboards.

Pupils:

- Curriculum iPads and desktops in the classrooms including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (e.g. Beebots, control equipment, class cameras 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.

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 Monkfield Park 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.

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials
- Our programme for e-safety education is evidenced in teachers' planning either as discrete or embedded activities.
- Key e-safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in discussion forums.

Continued Professional Development:

- Staff at Monkfield Park 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. Monkfield Park aim to provide e-safety training at least once every academic year.
- New staff receive information on the school's acceptable use policy as part of their induction, including advice on Protecting their Professional Reputation Online. E-safety is covered as part of induction alongside the acceptable use policy.
- 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.
- Staff are directed to the 'thinkuknow' website to receive training or updates relating to e-safety.

School website:

Schools are required to publish certain information online – which in practice means you must have a school website. You are not however required to develop a website policy but sometimes the boundaries of responsibility for setting up, maintaining and ownership of the content are blurred and this can lead to difficulty.

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 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.

Under safeguarding responsibilities, it is the duty of a school to ensure that every child in their care is safe, and the same principles should apply to the virtual presence of an educational setting as it would apply to its physical surroundings. The Headteacher and the Governing Body therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, a visitor using the school website.

Monkfield Park establishes clear procedures to ensure that its website is maintained, is effective, and does not compromise the safety of the pupils or staff.

Monitoring, and averting e-safety incidents:

Monkfield Park keeps children safe when using online technologies through a combination of e-safety education, filtering and monitoring children's online activity and reporting incidents, including following Child protection 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.
- Base line and enhanced filtering provided by the Lightspeed filtering system
- CPSN provided Sophos antivirus package
- Council funded email system for all school staff with direct internal routes to the council for trusted email communications.
- Restrictions on download of software, apps and file types from known compromised sites

Staff also monitor pupils' use of technology and, specifically, the internet.

- Pupils' use of online services (including the World Wide Web) are supervised in school at all times unless specific permission has been given for unsupervised use.
- Staff are also able to monitor pupils' activity in online learning environments, 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.
- 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 the Computing Subject Leader and visiting technician.
- School staff and pupils are not permitted to connect personal devices to the school's wireless network and visitors are granted access 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 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.

- Staff responses to e-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 e-safety incident occurs, Monkfield Park will follow its agreed procedures for responding 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.

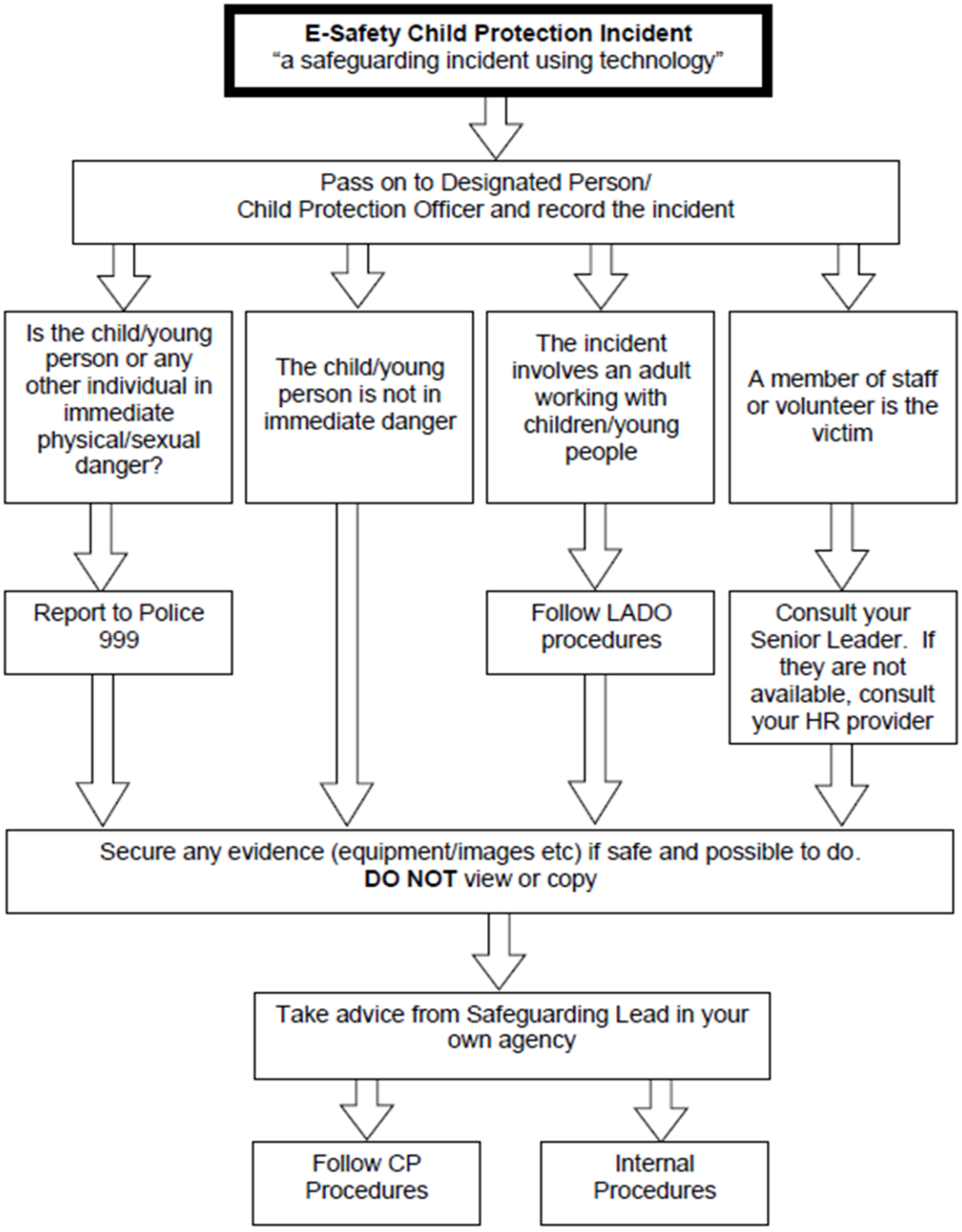
The Education Act 2011 gives school staff the powers, in some circumstances to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

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 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 …



Appendices:

1. Staff AUP
2. KS2 AUP
3. KS1 AUP
4. Reception AUP
5. SEND AUP

Apendix 1:

Monkfield Park 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
- Personal Mobile phones and devices
- Learning and teaching

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

Version Control

As part of the maintenance involved with ensuring your staff Acceptable Use Policy is updated, revisions will be made to the document. It is important that the document owner ensures the document contains the following information and that all revisions are stored centrally for audit purposes.

Title	Staff Acceptable Use Policy for Monkfield Park
Version	2.0
Date	22.11.2018
Author	ICT coordinator
Approved by headteacher	22.11.2018
Approved by governing body	22.11.2018
Next review date	Autumn 2019

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 e-safety coordinator.
- All passwords I create will be in accordance with the school e-safety Policy. 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/ Senior Information Risk Officer (SIRO) 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/ SIRO.
- 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/ SIRO (as appropriate)
- I understand my personal responsibilities in relation to the Data Protection Act 2018 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. If equipment is lost or damaged staff may be required to pay the insurance excess (£150) or 50% of the cost of replacement equipment dependent on circumstances.
- 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 protection2018 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 network manager/ SIRO.
- 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. Remote systems will only be accessed by authorised members of staff using secure logons and secondary authentication methods e.g. key fobs.
- 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 in a professional capacity and I will take all reasonable steps to ensure any online communication will not damage the schools reputation.
- I will set and maintain my profile on social networking sites to appropriate privacy levels and allow 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 e-safety 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 e-safety Policy/ Home School Agreement (or any other relevant policy).
- 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 take all reasonable precautions to ensure that any posts via electronic communication by myself 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 and ensure that the device has a pin code to access.
- 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.

Personal 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 and out of sight during the school day.
- Bluetooth, AirDrop and other wireless communication channels 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 Senior 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 of children or their work.
- I will my mobile/device in line with the school mobile phone, cameras and technological device policy.

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 technology 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 strive to 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:
Accepted by:
Date:

Appendix 2:

KS2 Acceptable Use Policy

- I will use the school's ICT equipment and tools 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 if a teacher or teaching assistant is 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 change 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 schools online 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 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 not bring in portable media e.g a mobile phone or memory stick from outside of school unless I have been given permission.

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 online communities or groups.
- Turn off my access for a little while.
- Not allow me access to use laptops / computers to access the internet or particular programmes.
- Take other action to keep me (and others) safe.

I am signing below to show that I understand and will try to abide by these rules

Name:_____

Signature:_____ Date:___/___/_____

I have read and discussed these rules with my child. I will support the school in ensuring my child follows these rules to keep themselves and others safe online.

Parent signature:_____Date___/____/_____

Appendix 3:

KS1 Acceptable Use Policy

- I will use the school's ICT equipment and tools (including computers, cameras, online environments e.g. Mathletics 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 and email when an adult is nearby.
- I will not share my passwords with other people and will tell my teacher if I think someone else knows them.
- I will ask an adult before opening an email from someone I don't know.
- I will not share details about myself such as surname, phone number or home address.
- I will ask if I need to change other peoples' work on the computer .
- I will try my hardest to only send messages which don't upset other people.
- I will ask my teacher before taking photos or video.
- If I see something on a screen which upsets me, I will always tell an 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, I know that my teacher may stop me using technology at school and talk to my parents about how I use technology.

Pupil's name:_____

Pupil's signature:_____ Date:_____

I have read and discussed these rules with my child. I will support the school in ensuring my child follows these rules to keep themselves and others safe online.

Parent signature:_____

Appendix 4:

Reception Acceptable Use Policy

- I will use the school's technology equipment safely and carefully.

- I will only use a program my teacher has said is OK.

- I will ask my teacher before taking photos or video.

- If I see or hear something on a screen which upsets me, I will always tell an adult.

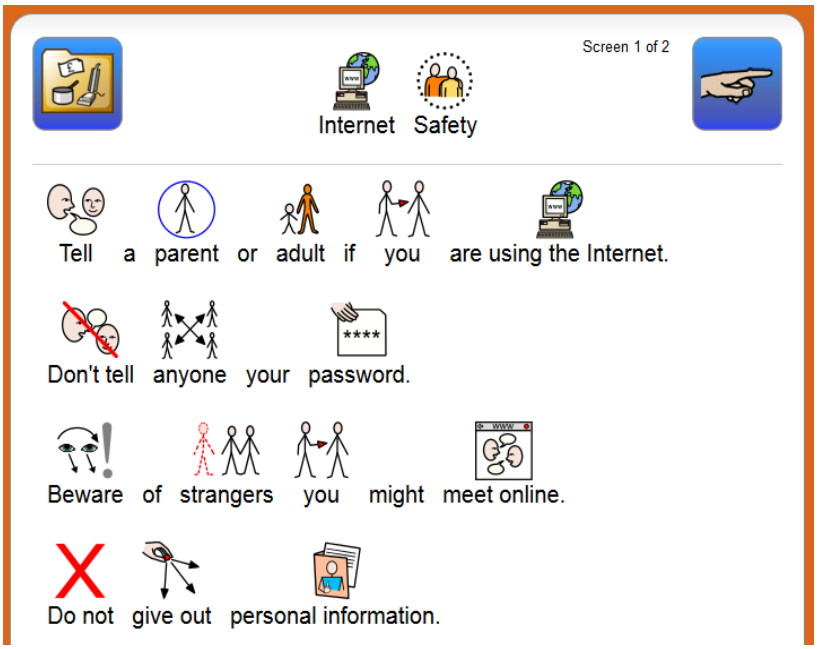
I will do my best to follow these rules because I know they are there to keep me and my friends safe. If I don't follow these rules, I know that my teacher may stop me using technology at school and talk to my parents about how I use technology.

Pupil's name:_____

I have read and discussed these rules with my child. I will support the school in ensuring my child follows these rules to keep themselves and others safe online.

Parent signature:_____Date___/____/____

Appendix 5:


Screen 1 of 2
Internet
Safety
Tell a parent or adult if you are using the Internet.
Don't tell anyone your password.
Beware of strangers you might meet online.
Do not give out personal information.


Do not send anyone a photo of you, your family or friends.
Tell an adult if you see anything worrying on the computer.
Do not chat to strangers on the internet.
Do not arrange to meet people you meet on the internet.
Star rating
5.0
Log in to rate an article
Log in to print