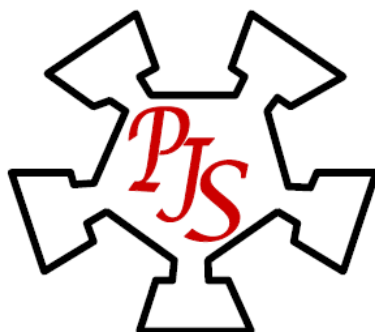


Priory Junior School



E-safety Policy

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 whole 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
- [School's Scheme of Work for Computing](#)
- 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 Person for Child Protection
 - The Computing Subject Leader
 - Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
 - Class teachers
- 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 a staff meeting, the Staff Share policies folder, and 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 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 Priory Junior 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 safely, responsibly and effectively and be able to critically evaluate, new technologies as they are developed

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, or radicalised, 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:

<p>Staff:</p> <ul style="list-style-type: none">IWBsLaptopsTabletsPCsCamerasCentral Hosting / SIMSSMART PhonesWi-fiSchool NetworkCloud-based resources <p>All members of staff have individual, password protected logins to the school network and some visitors to the school can access part of the network using a generic visitor login and password.</p> <p>The school is moving towards cloud-based document storage, with tight controls on levels of access.</p>	<p>Pupils:</p> <ul style="list-style-type: none">LaptopsTabletsIWBsPCsCamerasSchool Pupil NetworkWi-fiCloud-based resources <p>All pupils have year group log-ins to the school network, with individual log-ins, password protected to online software accounts.</p> <p>The school is moving towards individual log-ins, password protected to cloud-based document storage, and online software accounts.</p>	<p>Others visitors on school premises (agreed on a case-by-case basis):</p> <ul style="list-style-type: none">LaptopsTabletsIWBsWi-fi
---	---	---

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 school's network can either be accessed using a wired or wireless connection. The wireless network is encrypted to the standards advised by the Local Authority and the wireless key is kept securely by the Headteacher, Computing Subject Leader and the school office. School staff and pupils are not permitted to connect personal devices to the school's wireless network.

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 KS2:** use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

At Priory Junior 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 variety of online services. This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials including the ACE (Accredited Competence in E-safety) scheme of work and is linked to our online learning platform, Starz+.
- 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.
- Regular e-safety assemblies (termly).

Continued Professional Development:

- Staff at Priory Junior 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.

School website:

The school website is hosted by 'e-schools' and managed by the school, with support from The Education ICT Service. The website serves many purposes, including:

- Publishing the statutory information as required by the Department for Education
- Publishing school information for both existing and prospective parents
- Celebrating pupil achievement and sharing school news

In achieving these aims, the school will, from time to time, publish information about pupils, including news articles and photos. GDPR 2018 affects the use of information about pupils, including images. An image of a child is personal data and it is, therefore, a requirement, under GDPR, that consent is obtained from the parent of a child for any images made such as those used for school web sites, productions or other purposes. It is also important to take into account the wishes of the child, remembering that some children do not wish to have their photograph taken.

Photos will only be published in accordance with written parental permission (which is obtained at the start of each academic year). Care will be taken when posting images of children alongside other information

including examples of their work, awards and achievements. In accordance with Local Authority guidance:

- If the pupil is named, we will avoid using the photograph.
- If the photograph is used, we will avoid naming the pupil.

The school takes the storage and handling of personal data seriously, complies with GDPR principles and has a more detailed Data Protection policy available in school.

School's Facebook Page / Social Media Use:

The school makes use of a Facebook page for celebrating school events, and communicating with parents. As part of this, the following procedures apply:

- Photographs of children, and staff, will not be used on the page.
- Posts can only be created by the account holder, and appropriate security settings are in place.
- Staff are requested not to like or follow the page

Monitoring, and averting e-safety incidents:

The school 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 Protex filtering system
- CPSN provided Sophos antivirus package
- Monitored 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.
- Staff are also able to monitor pupils' activity in the Starz+ learning platform, 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. 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 and pupils are not permitted to connect personal devices to the school's wireless network and a guest wireless key is issued to visitors on a case by case basis.

The school is moving towards cloud-based systems for document storage – with individual, password protected logins for all staff, governors and pupils– and appropriate levels of access linked to them.

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, Priory Junior School 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.

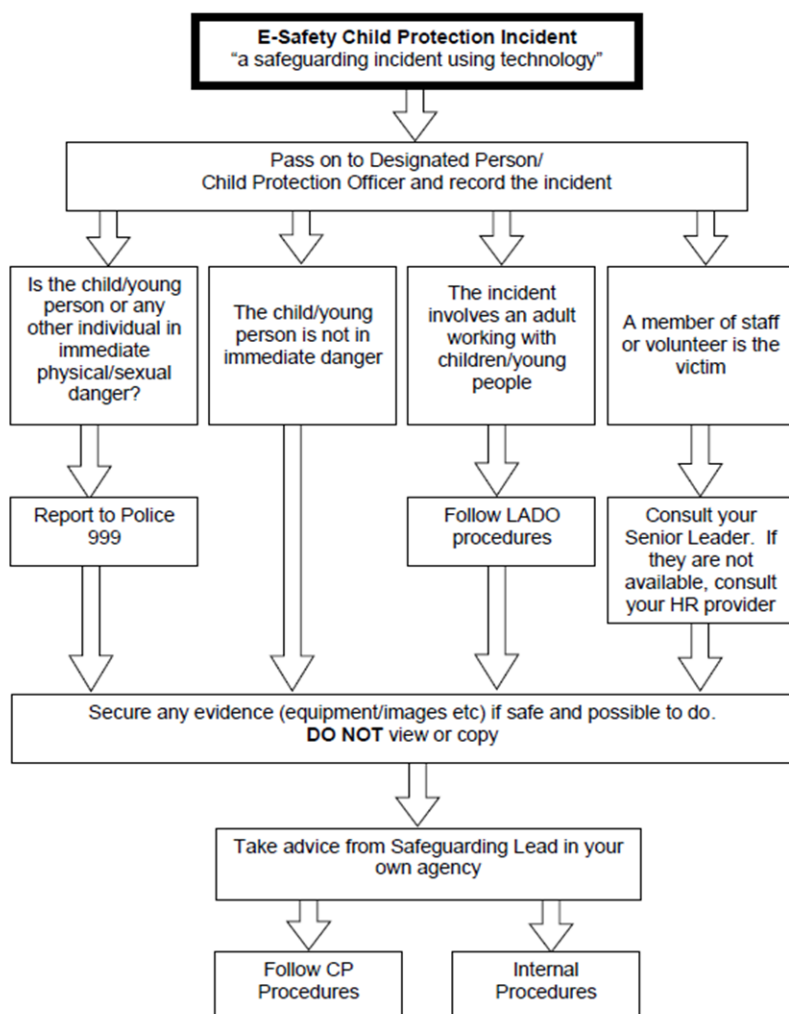
The Education Act 2011 gives school staff the powers, in some circumstances to search personal digital devices and decide whether or not to delete data or files if the person thinks there is good reason to do so.

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 ...



Agreed by governing body: 18/01/16

Reviewed November 2017

Reviewed November 2018

Signed.....

Date.....

Appendices:

- AUPs - staff, pupil, parents
- Risk assessments
- Incident Log
- E-Safety Curriculum Map

Priory Junior School
Pupil Acceptable Use Agreement



- ✓ 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 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 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 arrange to meet someone I have only ever previously met online. It could be dangerous.
- ✓ I will never post photographs or video clips of people I know without permission and never include names with photographs or videos.
- ✓ If I need to carry a phone (for the safety of my journey to and from school), I will hand it in to my teacher each day, and will not get it out at school events. I know I cannot bring it on school trips.
- ✓ I will support the school approach to online safety
 - 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 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 programs.
- 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

Signed.....

Date.....

Appendix 2

Dear Parent / Carer

The use of fixed and mobile technology, including use of online services such as communication and publishing tools (e.g. emails, blogs, discussion forums) and the World Wide Web continues to be an important part of learning in our school. We expect all children to be safe, respectful and responsible users of this technology and in partnership with them and you, work hard to keep them safe.

Please read and discuss these e-safety rules with your child and return their signed agreement and the slip at the bottom of this page. If you have any concerns or would like some explanation, please contact the school office or Head Teacher.



Parent / Carer signature

We have discussed this and(child's name)
understands the e-safety rules. We support the safe use of technology at Priory Junior
School by following these rules and will seek help / advice when unsure of what to do.

Parent/ Carer Signature

Class Date

Appendix 3

e-Safety Reporting Log

[illegible]

Appendix 4

Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

--




Web site(s) address / device

Reason for concern

Conclusion and Action proposed or taken

--

Appendix 5 - e-Safety Curriculum Map

	Year 3	Year 4	Year 5	Year 6
Curriculum Age-Expectations	<ul style="list-style-type: none"> I can talk about what makes a secure password and why they are important. I can protect my personal information when I do different things online. I can use the safety features of websites as well as reporting concerns to an adult. I can recognise websites and games appropriate for my age. I can make good choices about how long I spend online. I ask an adult before downloading files and games from the Internet. I can post positive comments online. 	<ul style="list-style-type: none"> I choose a secure password when I am using a website. I can talk about the ways I can protect myself and my friends from harm online. I use the safety features of websites as well as reporting concerns to an adult. I know that anything I post online can be seen by others. I choose websites and games that are appropriate for my age. I can help my friends make good choices about the time they spend online. I can talk about why I need to ask a trusted adult before downloading files and games from the Internet. I comment positively and respectfully online. 	<ul style="list-style-type: none"> I protect my password and other personal information. I can explain why I need to protect myself and my friends and the best ways to do this, including reporting concerns to an adult. I know that anything I post online can be seen, used and may affect others. I can talk about the dangers of spending too long online or playing a game. I can explain the importance of communicating kindly and respectfully. I can discuss the importance of choosing an age-appropriate website or game. I can explain why I need to protect my computer or device from harm. I know which resources on the Internet I can download and use. 	<ul style="list-style-type: none"> I protect my password and other personal information. I can explain the consequences of sharing too much about myself online. I support my friends to protect themselves and make good choices online, including reporting concerns to an adult. I can explain the consequences of spending too much time online or on a game. I can explain the consequences to myself and others of not communicating kindly and respectfully. I protect my computer or device from harm on the Internet.
	Term 1	Term 2	Term 3	Assessment, Achievements and Evaluation
Assemblies	Cyberbullying  I am kind and responsible	Personal safety  I am safe	Excessive/obsessive use  I am safe	Assessment Self and teacher assessments are on-going using Somerset Assessment resources, ACE resources, group/class I can poster
Theme weeks	Anti-bullying week includes cyberbullying messages.	Safer Internet Day is part of a week's focus on the use of the Internet, different devices and technologies.		Achievements ACE Awards are undertaken to children to recognise responsible behaviour.
Partnership with Parents and carers	Pupil/parent AUP and photo permissions for all new parents are signed. Leaflet sent home, copies of class agreed Internet rules sent home.	Children create leaflet/poster to take home for parents and carers.	A parent and carers assembly is led by children.	Evaluation Surveys of parents and carers, children and teachers are used to inform the planning for development of e-safety.
	An e-Safety meeting for parents and carers maybe planned, at the school or shared with other schools, where this is considered to be an effective strategy.			Information available on school website e-Safety news items included in newsletters

Appendix 6 - Risk Assessments

Activity / Event: Use of ICT			Date Assessed: 25/11/15			Priory Junior School		
Assessor's Name: Tracy Keefe / Daniel Folly			Assessment Ref. No.			Assessor's Signature:		
High Risk (Rate >7) – Unacceptable risk, take immediate action			Moderate Risk (Rate 4 – 6) - May or may not be an acceptable risk. Introduce & make all efforts to control/reduce risk			Low Risk (Rate 1- 3) – Risk may be acceptable, but consider possible low or no-cost improvements.		

A	B	C	D	E	F	G	H	J	K	L	M	N	P	Q	R
Hazards (the potential for harm) arising from activity / event	Can the hazard be eliminated or reduced?	Risks (Identify who may be harmed, how they may be harmed and how likely it is)	Risk level without controls			Existing controls (preventive and protective measures provided)	Risk level with existing controls			Risk level acceptable Y/N	Additional control measures required to reduce risk to acceptable level	Residual risk Level			Initials of Line Manager responsible for monitoring (G) and implementing (M)
			Likelihood (1-4)	Severity (1-4)	Risk Level (1-16)		Likelihood (1-4)	Severity (1-4)	Risk Level (1-16)			Likelihood (1-4)	Severity (1-4)	Risk Level (1-16)	
Accessing internet for research	N	Child / adult - Viewing inappropriate content including images - More than likely	4	3	12	Filtering system in school Child-safe search engines used Website links pre-prepared for lessons	1	3	3	Y	None	1	3	3	TK
Use of YouTube videos	N	Child / adult - viewing inappropriate content - bringing school into disrepute - more than likely	4	3	12	Youtube videos displayed using PureView only	1	1	1	Y	None	1	1	1	TK
Mathletics, Education City, Alfie-Soft, SPAG.com use	N	Child - Communication with strangers - More than likely	4	3	12	Software does not allow children to communicate with others	1	1	1	Y	None	1	1	1	TK
Scratch use	N	Child - Communication with strangers - More than likely	4	3	12	Be able to report comments left they don't like Agree to Scratch's e-safety agreement Delete comments they don't like	3	2	6	Y	Inform parents at the start of any Scratch project	2	2	4	TK
Sending emails / Creating online blogs	N	Child - Communication with strangers – unsecured - Inappropriate messages sent - More than likely	4	3	12	STARZ used – learning platform – only allows children to email within school community Whistle-blowing mechanism to report inappropriate messages Admin have access to view emails sent	2	2	4	Y	None	2	2	4	TK

Review Date	Review Date	Review Date	Review Date	Review Date
Signed Assessor	Signed Assessor	Signed Assessor	Signed Assessor	Signed Assessor