

St Helen's Primary School



Online safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The school's online policy will operate in conjunction with other policies including: Safeguarding and Child Protection Policy, Behaviour Policy, Anti-bullying Policy, Social Networking and Sites Policy, Computing Policy and Data Protection Policy.

It is essential that this policy shows the ability to:

- protect and educate pupils and staff in their use of technology
- have the appropriate mechanisms to intervene and support any incident where appropriate.

(Inspecting online safety in Schools, Ofsted 2012)

This policy considers guidance from:

- Teaching Online Safety in Schools guidance – DfE, June 2019
 - Education for a Connected World – UKCIS, June 2020
 - National Curriculum in England - Computing - DfE, Sept 2014
 - Relationships and Health Education – DfE, July 2020
-

Online Safety Policy

Contents

Background to this policy	2
Rationale.....	3
The online safety curriculum	4
Continued Professional Development.....	4
Managing Internet Access.....	5
Responding to online safety incidents.....	6

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 filtering, monitoring, and preventing and responding to online safety incidents
- A progressive, relevant age-appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education and **includes specific reference to the prevention of radicalisation**

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

- Personal Social and Health Education (PSHE)
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Whistle Blowing Policy
- **Prevent Action Plan**

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 online safety policy involved:

- The Headteacher
- The Designated Safeguarding Lead
- The Computing Subject Leader
- Use of online documentation on the Cambridgeshire Education ICT Service website
- Use of Purple Mash Toolkit for Computing Leaders
- The governor responsible for Safeguarding

It was presented to the governing body on and ratified on 5th May 2023 and will be formally reviewed in May 2024.

- 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 and through staff discussions and is readily available on the school network and website, and has also been made available to parents.
- 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 our school's approach to safeguarding, 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 St Helen's 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 misuse of technology 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 / desktops - staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR.
- Staff / some staff have access to school systems beyond the school building (e.g. MIS systems, cloud platforms e.g. Microsoft 365 or Google Workspace, Seesaw, Purple Mash, Tapestry).
- Class cameras and other peripherals such as visualisers, I-pads and Interactive Whiteboards
- Staff level internet access
- Social media e.g. Facebook.

Pupils:

- Curriculum laptops / iPads desktops including filtered access to the Internet and pupil level access to areas of the school network
- Cameras and peripherals including programming resources (beebtos, romas, probots etc)
- Cloud platforms / online tools providing pupils with access within and beyond the school gates (such as Seesaw, Tapestry, Purple Mash and TTRS)

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 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 (England) and the statutory Relationship and Health Education.

At St Helen's 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.

Our online safety curriculum has been compiled through the readings of documents such as the Cambridgeshire Progression in Computing Capability Materials, and the Cambridgeshire PSHE Service Primary Personal Development Programme, developing links into the curriculum with UKCIS's Education for a Connected World

This is achieved using a combination of:

- Discrete and embedded activities drawn from a selection of appropriate materials which demonstrate the use and need for safe practices whenever online.
- Key online safety messages are delivered and reinforced through cross curricular opportunities such as emailing, researching, blogging and communicating in appropriate online environments.
- Focus events to raise the profile of online safety for our pupils and school community. (Safer Internet Day)
- A flexible curriculum which is able to respond to new challenges as they arise.

Continued Professional Development

Staff at St Helen's Primary School receive information and training on online safety 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.

Managing Internet Access

Information system security

- If staff or pupils discover an unsuitable site, it must be reported to the class teacher who then is responsible for reporting to the school technician.
- Virus and Spyware protection will be installed and updated regularly.
- Login details must not be shared.
- SLT will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Email

- Pupils and staff may only use approved e-mail accounts in school.
- Pupils and staff must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Pupils and staff must treat emails with links or attachments as suspicious and not open any links unless they know they are safe.
- E-mails sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- Pupils will be taught how to report unpleasant Internet content.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- A pupil's full name will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

- The school's filtering system will block access to inappropriate social networking sites.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Staff must not communicate with students using public social networking sites such as Facebook, Twitter, tick,tock, snapchat etc.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- The inclusion of inappropriate language or images within text messages is difficult for staff to detect. Pupils may need reminding that such use is both inappropriate and conflicts with school policy. Abusive messages may be dealt with under the Bullying Policy.

Managing emerging technologies

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

Protecting personal data

- Personal data will be protected following the legal requirements of the Data Protection Act 2018.

Use of phones / mobile phones

- Staff must use a school phone where contact with parents/pupils is required.
- Staff will keep personal phones in their locker. They are not to be used in teaching sessions, but can be used in the staffroom at break times.
- Staff will not use their personal phone for photos or the Internet while in teaching session.
- Pupils are not allowed a mobile phone in class. If they bring a mobile to school (which a parent must agree to) they have to leave it in a teacher's drawer at all times during the school day. There is a separate letter for parents to agree to this.

Whilst we recognise that it is impossible to eliminate all risks associated with the use of technology, these safeguards are in place to help minimise these risks to an acceptable level.

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 must be taken in some circumstances.
- If an online safety incident occurs, St Helen's Primary School will follow its agreed procedures for responding including internal sanctions and involvement of parents (this may include the deactivation of accounts, restricted access to systems as per the school's AUPs or reporting incidents to the police and other authorities– 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 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.

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 Safeguarding issue, the usual Safeguarding procedures will be followed. This process is illustrated in the diagram below.

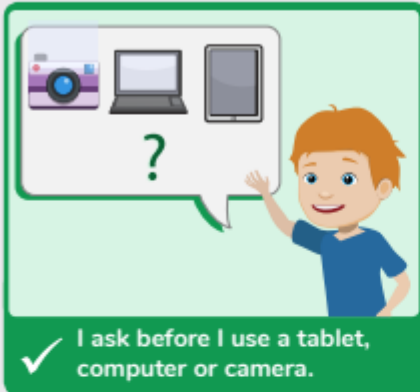
You come across a child protection concern involving technology ...

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



Acceptable Use Agreement

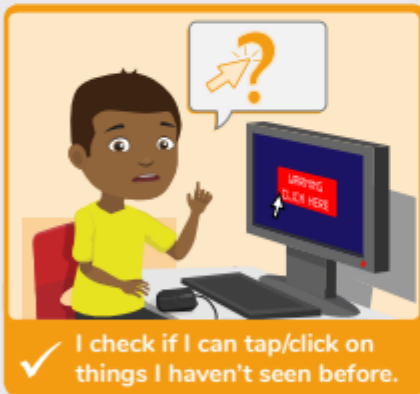
(For EYFS)



✓ I ask before I use a tablet, computer or camera.



✓ I tap or click on things I have been shown.



✓ I check if I can tap/click on things I haven't seen before.



✓ I tell a grown-up if something upsets me.

My Name:

Class:

Parent/Carer Signed:

Today's Date:



www.2simple.com
Raising Standards Through Creativity

Contact us

Tel: 0208 203 1781

Email: support@2simple.com



Acceptable Use Agreement

- ✓ I always ask a teacher or suitable adult if I want to use the computers, tablets or cameras.
- ✓ I only open activities that an adult has told or allowed me to use.
- ✓ I know that I must tell an adult if I see something on a screen that upsets me, or I am unsure of.
- ✓ I keep my passwords safe and will never use someone else's.
- ✓ I know personal information such as my address and birthday should never be shared online.
- ✓ I know I must never communicate with strangers online.
- ✓ I am always polite when I post to our blogs, use our email and other communication tools.

I understand this agreement and know the consequences if I don't follow it.

My Name:

Class:

Parent/Carer Signed:

Today's Date:



Acceptable Use Agreement

- ✓ I will only access computing equipment when a trusted adult has given me permission and is present.
 - ✓ I will not deliberately look for, save or send anything that could make others upset.
 - ✓ I will immediately inform an adult if I see something that worries me, or I know is inappropriate.
 - ✓ I will keep my username and password secure; this includes not sharing it with others.
 - ✓ I understand what personal information is and will never share my own or others' personal information such as phone numbers, home addresses and names.
 - ✓ I will always use my own username and password to access the school network and subscription services such as Purple Mash.
 - ✓ In order to help keep me and others safe, I know that the school checks my files and the online sites I visit. They will contact my parents/carers if an adult at school is concerned about me.
 - ✓ I will respect computing equipment and will immediately notify an adult if I notice something isn't working correctly or is damaged.
 - ✓ I will use all communication tools such as email and blogs carefully. I will notify an adult immediately if I notice that someone who isn't approved by the teacher is messaging.
 - ✓ Before I share, post or reply to anything online, I will T.H.I.N.K.
- T** = is it true?
H = is it helpful?
I = is it inspiring?
N = is it necessary?
K = is it kind?
- ✓ I understand that if I behave negatively whilst using technology towards other members of the school, my parents/carers will be informed and appropriate actions taken.

I understand this agreement and know the consequences if I don't follow it.

My Name:

Class:

Parent/Carer Signed:

Today's Date:



Acceptable Use Agreement

(Staff)

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. Digital technologies give staff opportunities to enhance children's learning in their care and enable staff to become more efficient in their work. The very nature of digital technologies means that they should be used with care and particular attention given to demonstrating appropriate behaviours and avoidance of misuse at all times.

Professional integrity and strong moral purpose must be upheld at all times by staff. It is the duty of all staff members to ensure that children in their care get the very best start to the world of digital technology. This should include provision of a rich, robust online safety education for the children with clear reporting procedures for infringements to safeguarding. Having a transparent approach to using digital technology is a must. Additionally, staff should develop critical thinking in their children, along with strategies for avoiding unnecessary harm and strategies for dealing with online safety infringements.

The school's internet, network and ICT systems and subscriptions to services should be used with the utmost professionalism at all times. The school will aim to provide its staff with secure systems which will have filtering, monitoring and virus protection included. Anyone with access to the systems should be aware that their use of the systems is monitored, and this can be used to form evidence should any suspected infringements occur.

Acceptable Use Agreement

By signing this agreement, you will have access to the school's systems and acknowledge that you agree to all the statements below. Additionally, that you have read and understand school policies which have a bearing on this agreement.

- I will demonstrate the value of the use of digital technologies in improving the outcomes for children in my care.
- I will educate children in my care about the safe use of digital technologies, acting on any online safety issues in accordance with the school's policies.
- I understand my use of the school's ICT systems/networks and internet are monitored.
- I recognise that whether within school or out of school, I must abide by the rules/statements set out in this document when using systems, accessing/transferring data that relate to the school or impact on my role within the school and wider community.
- I know what GDPR is and how this has a bearing on how I access, share, store and create data.
- Any data that I have access to away from school premises must be kept secure and used with specific purpose. As outlined in the school's data protection policy, it is my responsibility to ensure when accessing data remotely that I take every bit of reasonable care to ensure the integrity and security of the data is maintained.
- I understand that I am fully responsible for my behaviours both in and out of school and as such recognise that my digital communications, subscriptions and content I access can have a bearing on my professional role.
- I recognise that my social media activity can have a damaging impact on the school and children in my care at school if I fail to uphold my professional integrity at all times whilst using it.
- If I am contributing to the school's social media account(s) or website(s) I will follow all guidelines given to me, with particular care given to what images/video imagery and details can be uploaded.
- I will never upload images/video imagery of staff/pupils or other stakeholders to my personal social media accounts unless there is significant reason to and that permission has been granted by the headteacher in writing for each occurrence.
- I will inform the school at the earliest opportunity of any infringement both on and off site by myself. Furthermore, if I am concerned about others' behaviour/conduct, I will notify the school at the earliest opportunity.
- I will never deliberately access, upload or download illegal, inflammatory, obscene or inappropriate content that may cause harm or upset to others.
- I will never download or install software unless permission has been given by the appropriate contact at school.
- I shall keep all usernames and passwords safe and never share them. Writing down usernames and passwords, including storing them electronically, constitutes a breach to our data protection and safeguarding policy.
- I will never leave equipment unattended which could leave data and information vulnerable; this extends to accessing data/services/content remotely.
- Any personal devices I own shall not be used to access school systems/data/services/content remotely unless I have adequate virus protection and permission from the school.
- I understand that mobile devices, including smart watches, shall not be used, nor in my possession, during times of contact with children. These devices will be securely locked away with adequate password protection on them should they be accessed by an unauthorised person.
- Any school trips/outings or activities that require a mobile phone/camera will be provided by the school and any data collected on them will be used in accordance with school policies.
- At no point- will I use my own devices for capturing images/video or making contact with parents/carers.

Staff Name:

Signature:

Date:



www.2simple.com

Contact us

Tel: 0208 203 1781



Acceptable Use Agreement

(For Parents/Carers)

Background and purpose

With access to rich dynamic content, connectivity across the globe, a platform for creativity and a place to engage in debate, digital technologies provide a powerful tool for learning. It is therefore essential that children are fully equipped to have the skills and knowledge to safely access and use digital technologies.

This **Parent/Carer Acceptable Use Agreement** is intended to help share the importance that the school places on keeping children safe with particular regard to online safety. It additionally intends to encourage parents/carers to be actively involved in their child's online safety education, including encouraging transparent behaviour, critical thinking and reporting.

The school will aim to provide every child with the best access it can to online technologies. Filtering, monitoring and alert systems will be in place to help protect children from unnecessary risks. The school will actively encourage children to think critically about content and communication from others and develop strategies for recognising inappropriate content/behaviours and how to deal with them. In return, the school expects the children to demonstrate that they are responsible users of digital technologies at all times.

Parents/Carers

We ask parents and carers to support us by:

- ✓ Sharing good online behaviours with your child.
- ✓ Emphasising the importance of the Acceptable Use Statements/School's rules your child has agreed to.
- ✓ Highlighting the importance of accessing only age-appropriate content and sites along with the pitfalls of social media.
- ✓ Explaining how to keep an appropriate digital footprint.
- ✓ Discussing what is and isn't appropriate to share online.
- ✓ Emphasising never to meet anyone online nor trust that everyone has good intentions.
- ✓ Reporting any concerns you have whether home or school based.
- ✓ Stressing the importance of openness when being online and that no one should ever be too ashamed or embarrassed to tell a trusted adult if they have seen/shared anything concerning or have had inappropriate online contact.
- ✓ Drawing up an agreement of online safety rules for outside of school that are applicable even when your child is at a friend's home.
- ✓ Avoiding posting or replying to any comments about the school to social media that may have a negative impact. Any concerns or worries should be reported to the school in the first instance.

Permission Access

By signing below, you agree to allowing your child access to the school's internet and ICT systems. This also includes any educational subscription services. You are also aware that your child has signed/agreed to the school's Acceptable Use Agreement for pupils.

Your Child's Name:

Class:

Parent's/Carer's Signature:

Date:

*The school aims to comply with GDPR regulations at all times and as such follows strict protocol about how we use personal data and keep it safe, including the information on this form. It is important that you refer to the school's data protection policy or contact the school if you have any questions about data.



www.2simple.com

Business Standards. Transform. Creativity.

Contact us

Tel: 0208 203 1781