Glebelands Primary Academy

Online Safety Policy
2025-26

Last Review Date: Autumn 2025
Next review Date: Autumn 2026

Background to the Online Safety 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 practices embedded in our school and followed by the whole school community
- The infrastructure and how it is set up to keep pupils safe online, including monitoring and preventing and responding to online safety incidents
- A progressive, relevant age-appropriate online safety curriculum for all pupils which (as a minimum) meets the requirements of the National Curriculum for Computing and the statutory Relationships and Health Education

Online safety in schools is primarily 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)
- Teaching Online Safety in Schools guidance – DfE, Updated 2023
- Safer Working Practices
- Data Protection / GDPR Policy
- Anti-Bullying Policy
- School Complaints Procedure
- Teach Computing Materials
- Whistle Blowing Policy
- Education for a Connected World – UKCIS, June 2020
- National Curriculum in England - Computing - DFE, Sept 2014
- Relationships and Health Education – DfE, July 2020
- Searching, Screening and Confiscation – Advice for schools – DFE, 2023

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 Online Safety Policy and its implementation will be reviewed every year or more frequently if needed. This policy may also be partly reviewed and/or adapted in response to specific online safety incidents or developments in the school's use of technology. It has been shared with all staff via email, is available on the school website or as a paper copy from the school office. The development of our online safety policy involved:

- The Headteacher
- The Designated Safeguarding Lead
- Online Safety Lead
- The Computing Subject Leader
- Cambridgeshire Local Authority Advisor (Cambridgeshire Education ICT Service)
- The governor responsible for Safeguarding

It was presented to the governing body on_____ and ratified on _____ and will be formally reviewed in September 2026.

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

Rationale

At Glebelands Primary Academy, 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 face can be broadly categorised into the '4C's': **Contact, Content** and **Conduct** (Livingstone and Haddon) with a more recent fourth 'C', Commerce, also being added 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, including strangers
• Cyber-bullying
• 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
• Phishing or financial scams
• 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. 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.

The Online Safety Curriculum

At our school, we believe that a comprehensive programme of online safety education is vital for developing our pupils' ability to use technologies safely. This is achieved through a combination of discrete and embedded activities. Our programme of online education will be evidenced in teachers' planning either as discrete or embedded activities.

We have planned a range of age-related teaching and learning opportunities to help our pupils become safe and responsible users of new technologies. Pupils will be taught online safety lessons throughout the year following Teach Computing; PSHE units of work and in line with the Computing Curriculum 2014.

The need for a progressive age-appropriate online safety curriculum is clearly documented in the 2014 Computing Curriculum, which states that:

At Key Stage 1:

- children 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 Key Stage 2:

- children use search technologies effectively, appreciate how results are selected and ranked, and are discerning in evaluating digital content
- children use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behavior; identify a range of ways to report concerns about content and contact

By the end of primary school, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality internet access as part of their learning experience. Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Benefits of using online technologies in education include:

- Access to worldwide educational resources
- Access to experts who would otherwise be unavailable
- Access to anytime, anywhere learning
- Collaboration across schools, networks of schools and services

Internet use will enhance learning:

- The school internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils
- Pupils will be taught what internet use is acceptable and what is not and given clear objectives for internet use
- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation

Pupils will be taught how to evaluate internet content. 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 may make them feel uncomfortable.

- The school will ensure that the use of internet derived materials by staff and pupils complies with copyright law
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Some of the activities the children will take part in will include:

- Online Safety assemblies
- Specific activities during Safer Internet Day (February) and Anti-Bullying week (November)

- Age-related classroom activities using a wide range of resources including: ThinkUKnow materials, Purple Mash materials, National Online Safety materials
- Related work in PSHE lessons (ESafety units)
- Teach Computing
- Posters and reminders around the school

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or Facebook group. This policy will also be available on our website.

The school will let parents know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the head teacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the head teacher.

School website/Facebook

The main purpose of our school website and Facebook (closed group page) is to provide information. Our school website will not only tell the world that our school exists, but it will provide information to our pupils and parents, promote the school to prospective ones and publish, as a minimum, the statutory information required by the Department for Education. In conjunction with a range of online services, our school website can be used to showcase examples of pupils' work - in words, pictures, sound or movie clips - and can share resources for teaching and learning both within the school and with colleagues elsewhere.

Under safeguarding responsibilities, it is 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 a school as it would apply to its physical surroundings. Headteachers and the Governing Body should therefore take on the responsibility to ensure that no individual child can be identified or contacted either via, or as a result of, information displayed on the school website/Facebook group. The school has established clear policies to ensure that its website is maintained, is effective, and does not compromise the safety of the pupils or staff.

Members of staff at Glebelands Primary Academy and the DLPT have access to the school website. Teachers are responsible for ensuring class pages are updated; subject leaders ensure documentation for their subject is up-to-date and reviews of all information shared are regularly undertaken. The website is hosted by Primary Site and an annual review of all content takes place.

Publishing pupils' images and work

- Photographs/videos that include pupils will be selected carefully and will not have their names printed with them
- Pupils full names will not be used anywhere on the website/Facebook, particularly in association with photographs/videos
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website/Facebook
- Pupils' work can only be published with the permission of the pupil and parents.

Monitoring and averting online safety incidents

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

The school's technology infrastructure is designed to minimise the risks associated with adult and pupil use of technology. This is provided and maintained by both an internet provider and Joskos. Safeguards built into the school's infrastructure include:

- An enterprise-class Sophos XGS firewall that provides firewalling, safeguarding (IWF, CTIRU) filtering, restrictions on download of executable files, malware and IPS detection, managed by our Internet Service Provider and kept up to date during the lifecycle of the firewall.
- • Age-appropriate, user-based filtering for staff and students to ensure appropriate access to websites.
- Antivirus package provided as part of a broadband connection
- Email system for all school staff through Microsoft Exchange, secure mail servers are accessed through Office 365
- Wireless networks installed are encrypted to industry best-practice standards and the wireless key should be kept securely by the school office

Staff also monitor pupils' use of technology and, specifically, their activity online. This is achieved through a combination of:

- Appropriate levels of supervision when pupils are using online technologies
- Auto-generated alerts which flag up activity in specific safeguarding categories which may raise child protection concerns
- Use of additional reporting tools to monitor and investigate pupil use of the Internet.

Staff use of the schools' internet can also be monitored and investigated where needed.

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 / cloud service / MIS systems
- Visitors to the school can access part of the school systems using a generic visitor login and password
- The wireless network is encrypted to the standards advised 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, unless express permission is given, and a wireless key is issued to visitors 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 to an acceptable level.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their classes.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate. All staff, governors and volunteers (where appropriate)

receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Technology at Glebelands Primary Academy

Technology regularly used by pupils and stakeholders include:

Staff:

- Laptops and desktops, iPads – staff devices can also be used at home in accordance with the staff AUP, particularly with regard to GDPR
- Cameras, Video cameras, Visualisers, USB microphones and headsets
- Interactive whiteboards
- Staff-level internet access
- Some staff have access to school systems beyond the school building: e.g. e-mail, Purple Mash, Arbor, school website, Grammarsaurus, Twinkl, Times Table Rockstars, Facebook

Pupils

- Laptops and desktops, iPads and Tablets
- Cameras, video cameras, visualisers, USB microphones and headsets
- Interactive whiteboards
- Pupil-level (filtered) access to the internet and areas of the school network
- Cloud platforms and online tools providing access within and beyond the school gate e.g. Purple Mash and Office 365 Education, including email, discussion forums, blogs and other communication tools, LBQ and Times Table Rockstars Facebook (with the teacher only)
- Other peripherals such as programmable toys, dataloggers, control technology equipment

Mobile phones will only be used during non-contact time and away from the children. The sending of abusive or inappropriate text messages is forbidden.

We recognise that when children begin to walk to and from school independently, they may bring a mobile phone to school. If they bring mobile phones to school, these are to be switched off upon arrival and handed in to be stored in a safe place until they leave. No child should be using a mobile phone on school premises.

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

Continued Professional Development

Staff at Glebelands Primary Academy receive up-to-date information and training on online safety issues in the form of staff meetings and updates from the school's online safety and Designated Safeguarding Leads, as well as training from external providers where appropriate.

- Nominated members of staff receive more in-depth online safety training to support them in keeping them 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.

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. The Online Safety Lead is Nicola Folwell – Deputy Head (also a DSL). The Online Safety Lead holds responsibility for liaising with Wave9 regarding monitoring and filtering arrangements.

- Staff responses to online safety incidents must be consistent with responses to other incidents in school. My Concern will be used to log concerns where necessary. This may mean that serious actions must be taken in some circumstances.

If an online safety incident occurs, Glebelands Primary Academy 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 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 she deems it appropriate.

The Education Act 2011 gives school staff the powers, in some circumstances, to search personal digital devices and decide whether to delete data or files if the person thinks there is good reason to do so.

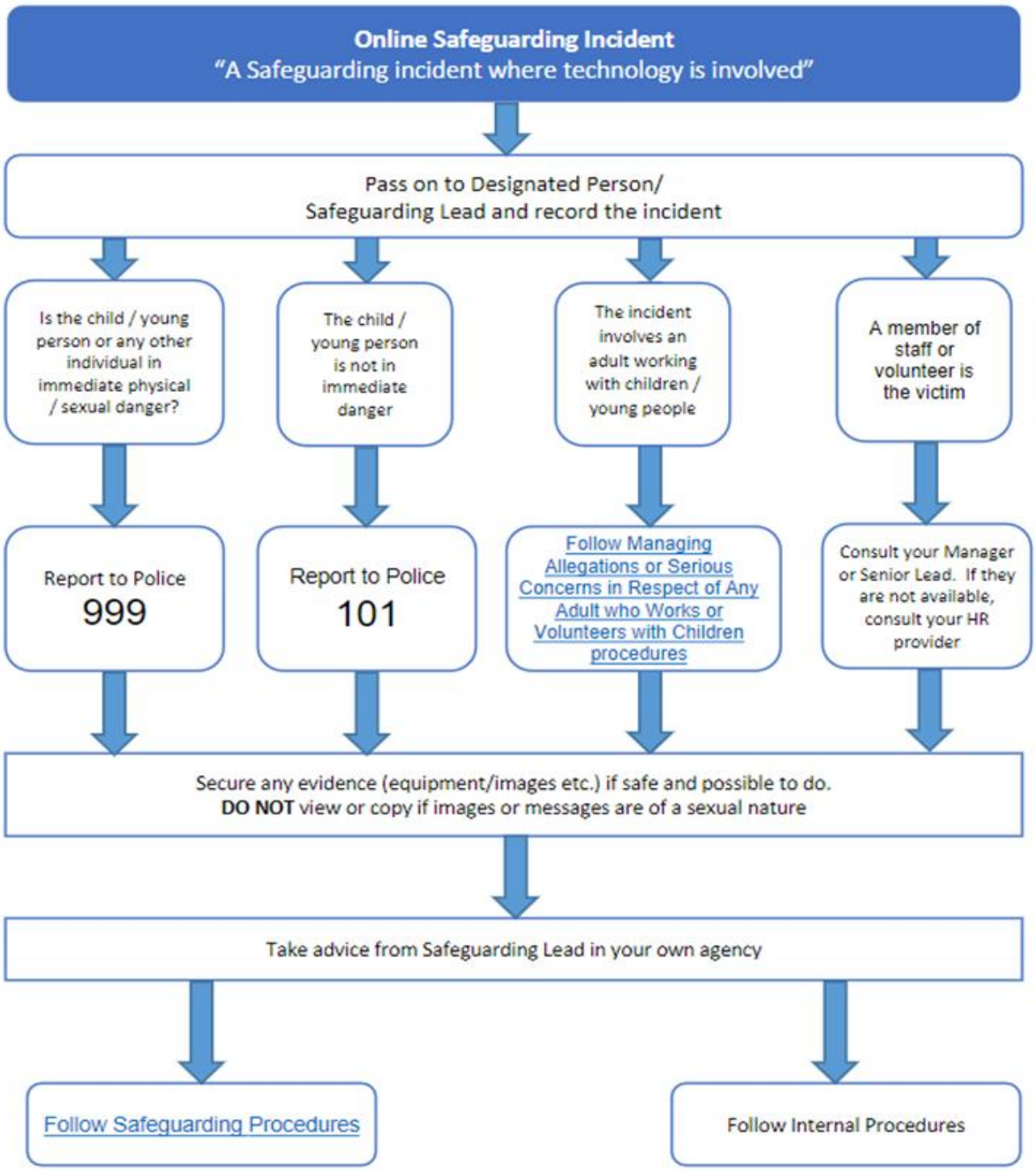
However, there is a risk that this could conflict with guidance about dealing with incidents where a child may be at risk where it may be inadvisable to delete, save or share content. The school will always seek to resolve areas of concern in line with safeguarding procedures, and with parents where appropriate, before taking any further action.
NB: In our school, the likelihood of these types of instances occurring are already reduced as we do not allow pupils to use personal devices in school.

If a pupil does need to bring a mobile device into school, this device is to be switched off and taken to the office at the beginning of the day, where it will be placed in a locked drawer to be collected at the end of the day.

Where the school suspects that an incident may constitute a safeguarding issue, the usual safeguarding procedures will be followed – see appendix 1.

Appendices:

You come across a Safeguarding concern involving technology …



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

If you think that a child or young person is at risk of serious harm contact Children Social Care

https://safeguardingcambspeterborough.org.uk/concerned/

Out of hours emergencies 01733 234724.

Acceptable use of the school's ICT facilities and the internet:
agreement for staff, governors, volunteers and visitors

Name of staff member/governor/volunteer/visitor:

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms unless they are to do with school business
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote any private business, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.
I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	Date:

Dear Parents,

At Glebelands Primary School, we have access to Office 365 Education, including Teams and Purple Mash.

These programs have many components that enable children to practise, safely, skills they will need for the future. Each pupil will be given their own log-on and they will have a username and a confidential password. Key Stage One children will have a password to share with their parents whilst Key Stage Two will be expected to keep their passwords completely confidential. Being web-based, these programs can be accessed and used both in school and at home. For this reason, I would encourage you to talk to your children about their accounts and how they use them.

Office 365 for Education provides a wealth tools, including the ability to communicate, save work, use Microsoft programs, such as Word and One Note, and the ability to converse with others in their class. Purple Mash gives the children further communication methods in the form an email account. The children will be able to save files to both platforms. The file storage areas in each will enable children to access work at home that has been saved here at school for a variety of reasons: sharing work with parents, a piece of work started at school could be available for continuing at home and vice versa. Teams and One Note Class Notebook (365 Education) also gives the opportunity for the children to collaborate on pieces of work, which is an amazing way to complete virtual group work.

These programs have been developed with safety as a main priority for children. All Purple Mash children accounts will include the "Safemail" system. This means that irrespective of whether a pupil is sending an email from home, school or wherever, they can only use it to send messages to other people within Glebelands. They can only receive messages from others within the school; external messages are never received by the pupil. Attempts to send messages to external email addresses are blocked from pupil accounts. Pupils may only email outside of the school by first sending the message to the teacher, who will read it, and then may or may not forward it to the recipient; any replies would also be passed through the teacher. All communication on pupils' accounts can and will be monitored by staff periodically and the children are aware that any misuse or abuse will result in instant barring from its use. Each pupil will also agree a User Agreement before being given their username and password.

In class, the use of these platforms has been discussed, focusing on:

Personal responsibility: internet services, are provided by the school as an education tool. They are a privilege, not a right. Personal use of the service is acceptable provided pupils behave responsibly.

Identity theft: Do not give anyone else, including family members (unless KS1), your username or password details. If you do, that person may then pretend to be you.

Monitoring: School staff can and will look at emails, files stored on the system, etc.
You will be held responsible for everything that is found in your area; see 'Identity theft' above. Even deleted emails can be retrieved in serious cases.

Reporting: If you feel uncomfortable about anything that you find, any messages you receive etc., report it to a teacher or parent as soon as possible.

Sanctions: What will happen if you misuse the system; removal of account – fixed or for a period of time.

Once your child has their username and password, please encourage them to show you the platforms and what wonderful tools they are. Share in the excitement of being able to view some of their work from school either at home or using a computer at the public library together.

Online learning platforms have a vital role in keeping children safe whilst practising their digital skills. These platforms enable a safe environment, which teaches them how to develop positive online behaviours whilst having fun!

If you should have any queries regarding the platforms or your child's account, please do come and speak to me.

Yours sincerely,

Miss Butler
Computing Subject Leader

KS1

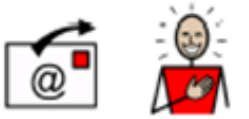
KS1 Acceptable Use Policy

I will use the school's ICT equipment and tools (including computers, tablets, cameras, Purple Mash etc.) for school work and homework.

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 try my hardest to only send messages which don't upset other people.

I will ask my teacher before using 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.

KS2 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 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.

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 password at any time.

I will only open email attachments from people who I know or an adult has approved. If I am unsure about an attachment or email, I will ask an adult for help.

I will not give out 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, email 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 programmes
- Take other action to keep me (and others) safe

6. Glossary

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

Term	Definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can

Term	Definition
	use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly- targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.