Old Basing Infant School.
Online Safety Policy.

UNCRC

Article 13 - **Children h**ave **the right to get and to share information**, as long as the information is not damaging to them or others.

Article 17 – Children have the right to reliable information from mass media. Television, radio and newspapers should provide information that children can understand and should not provide materials that could harm children.

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, misinformation, disinformation (including fake news), conspiracy theories, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit the user for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety
- Meeting digital and technology standards
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education (RSE) and health education (REHE)

- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and Responsibilities

The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board will make sure that the school teaches pupils how to keep themselves and others safe, including online.

The governing board will make sure that the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE's filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet the school's safeguarding needs

All governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 3)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-school or college approach to safeguarding and related policies and/or procedures
- Make sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

The headteacher

The headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies (DDSLs) are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy every 3 years and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety (appendix 4 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a fortnightly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by reporting this to HSS/School Safe (See Managing Information Systems section above).
- Following the correct procedures by HSS/SchoolSafe if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy

- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendices 1 and 2)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 3).

Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum

The text below is taken from the National Curriculum computing programmes of study and the government's guidance on relationships education, relationships and sex education (RSE) and health education (for teaching until 31 August 2026).

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- 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

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/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (Tapestry). This policy will also be shared with parents/carers. Online safety will also be covered during Curriculum Evening.

The school will let parents/carers 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/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Mobile Phone Use – Staff and Visitors to the school site

Old Basing Infant school strictly prohibits the use of personal mobile phones or cameras in child-facing areas to ensure safeguarding. Only school-owned devices are used for capturing images (e.g., learning journeys), which are stored securely and monitored and deleted at the end of each school year.
Staff, volunteers, and visitors must store personal devices away from children.

Visitors/Parents: Visitors are forbidden from using phones within the setting, including taking photos of their own children without consent.
Outings/Trips: Staff must use school-provided phones/tablets for emergencies and documentation, rather than personal devices.
Data Protection: Photos are only taken with parental consent. Images are deleted from devices promptly after being moved to the school's secure server.
Social Media/Sharing: Staff are prohibited from uploading any photos taken at the school to personal social media accounts, ensuring all images comply with GDPR regulations.

If an allegation is made regarding a staff member's improper use of technology, there is a clear safeguarding protocol for immediate reporting to the designated lead, often resulting in disciplinary action.

Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Gemini.
Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff. Any use of AI should be carried out in accordance with our AI usage policy.

Acceptable use of the internet in school

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 to 3). Visitors will be expected to read and agree to the school's terms on acceptable use, if relevant.
Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.
More information is set out in the acceptable use agreements in appendices 1 to 3.

Pupils using mobile devices in school

Pupils may not bring mobile devices into school.

Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use, as set out in appendix 3.
Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the Computing Lead.

How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour, the acceptable use of IT and the Social Media policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct and disciplinary procedures where appropriate. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training for staff, governors and volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in appendix 5.

This policy will be reviewed every year by the Computing Lead. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- ICT and internet acceptable use policy
- Social Media Policy

Why Internet use is important

- The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.
- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for children.
- 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.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries
- inclusion in the wider network of all UK schools
- educational and cultural exchanges between pupils world-wide
- vocational, social and leisure use in libraries, clubs and at home
- access to experts in many fields for pupils and staff
- professional development for staff through access to national developments, educational materials and effective curriculum practice
- collaboration across support services and professional associations
- improved access to technical support including remote management of networks and automatic system updates
- exchange of curriculum and administration data.
- access to learning wherever and whenever convenient.

How can Internet use enhance learning?

- The school's Internet is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and ability.
- Pupils are educated in the effective use of the Internet for research, including the skills of knowledge location, retrieval and evaluation.

How will pupils learn how to evaluate Internet content?

- Our school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The evaluation of on-line materials is a part of every subject.

Managing Information Systems

- The Business Manager is responsible for the management of our network with the support of HSS/School Care from February 2021
- Virus protection is updated regularly through automatic internet downloads which are remotely authorised by School Care/HSS.
- Security strategies will be discussed with the School Care /HSS team
- Portable media is checked automatically when opened by our virus protection software.
- Unapproved system utilities and software will not be allowed in pupils' work areas or attached to e-mail.
- Files held on the school's network are checked by our virus protection software on opening.
- The School Care /HSS team checks the health of the server hard drives remotely on a regular basis.
- HSS /School Care back up the network and server daily.

Filtered access to the World Wide Web

We are connected to the internet through School Care/ HCC. As part of this internet connection, some websites are filtered out as being deemed inappropriate. The filtering of the World Wide Web is a two-stage process. Information requested from the Internet must pass through both stages before it will be sent through to the school.

Stage 1 - Deny Lists: Whenever someone in a Hampshire school types in a World Wide Web address, or clicks on a link to an address, the request for that information is first passed to a computer, called a proxy server, at the centre of the School Care/HSS EdICT core network. This computer checks to see if the requested address is listed as being unsuitable. If it is on the list, instead of seeing the requested page the user will see a message indicating that the material on that page is thought to be inappropriate for use in schools. These deny lists are updated automatically every few days.

Stage 2 - The Dictionary: If it is not listed the page will be retrieved from wherever it may be on the Internet but as it comes back through the central computer the words contained on that page are checked. Certain words have a score associated with them and if the total score for any page reaches a given total then that page will not be sent through to the requesting school. Once again a message indicating the unsuitability of the material on that page is sent to the user instead.

However, the School Care/ HSS EdICT filtering cannot be 100% perfect because different people will draw the line about what is suitable and unsuitable for schools in different places and because the Internet changes so quickly that it is difficult to keep the deny lists up-to-date. The School Care/ HSS EdICT proxy server records all the websites visited. Our pupils are instructed that if they come across an internet page which they find distasteful, uncomfortable or threatening, they are to close the page and report it to their teacher immediately. He/she will arrange for the School Care /HSS EdICT Helpdesk to be contacted – they will be able to instantly add the page to the deny lists. Any material that the school believes is illegal is referred to School Care /HSS EdICT and the Police if appropriate. The school will work in partnership with School Care / HSS EdICT, to ensure systems to protect pupils are reviewed and improved.

How is e-mail managed?

Staff are provided with a HANTS webmail e-mail account. All inbound email is scanned for viruses and unsolicited mail (spam) before delivery. Staff should only be using these e-mail accounts and not personal e-mail accounts for any correspondence related to their role in school. Other e-mail providers may not provide strict filtering systems to protect from SPAM and viruses.

The security of the school's email service is ensured by School Care /HSS by:

• The structure of the addresses themselves

• The prevention of "spam" - Spam refers to all of the unsolicited junk e-mail that can clog up people's mailboxes once their addresses have been obtained from various sources. Our e-mail service is able to detect most spam messages by looking for certain key words and phrases which usually characterise them. If detected these spam messages are not delivered.

• The filtering out of computer viruses - If a message contains a computer virus this will be detected by the e-mail system and the message will not be delivered. Both the sender and the intended recipient will be automatically informed of what has happened.

Sensible Precautions

Nevertheless, there are still some basic precautions which staff should always take.

- If an e-mail is from an unknown sender delete it and do not open it.
- E-mails that contain rude or offensive content should not be sent via these addresses.
- If you receive an e-mail from someone you know, which you suspect may contain rude or offensive material this should not be opened on any networked school computer or laptop.
- If accessing e-mail using a computer accessible to any pupils ensure you are logged off before leaving the computer unattended.

Precautions taken by pupils and staff when e-mail is used within the curriculum.

- Children in Old Basing Infant School do not have their own school email account.
- E-mail sent to an external organisation should be written carefully and professionally in the same way as a letter would be written on school headed paper.
- E-mail received from an external organisation should be checked carefully by an adult before it is opened by pupils.
- Pupils must not reveal details of themselves or others, such as address or telephone number, or arrange to meet anyone in e-mail communication.
- Social e-mail use is not allowed.
- Access in school to external personal e-mail accounts may be blocked.

How is content on our school website managed?

- The contact details on the website are the school address, e-mail and telephone number. Staff or pupils' personal information must not be published.
- The Headteacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- The website should comply with guidelines for publications including respect for intellectual property rights and copyright.
- It is the responsibility of the adult uploading material onto the website to ensure that it does not infringe any copyright laws.
- Publication of images of children on the school website – Parents are asked to fill in a permission form to state whether publication of an image of their child is granted. This form is to be filled in when their child starts our school. No images of children are to be published accompanied by their name. As soon as a child leaves this school images will be deleted.

How is Internet access authorised?

- Access to the Internet will be by adult demonstration and supervised access to specific, approved on-line materials.
- All Internet materials will be reviewed and checked before pupils are allowed to use these.
- When pupils are using the internet to research it is advised only child appropriate search engines are used e.g. Kiddle.
- When pupils are using the Internet to research they should be directly supervised at all times.

How are risks assessed?

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor School Care/ HSS can accept liability for the material accessed, or any consequences resulting from Internet use.
- If a child does access unsuitable material this will be reported to the head teacher and ICT technician who will report it to HCC/School Care so this website can be added to the deny lists. The child's parents will also be informed.
- The school audits ICT use to establish if this E-safety policy is adequate and that the implementation of the E-safety policy is appropriate.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- This policy identifies the methods used to identify, assess and minimise risks. It will be reviewed annually with all staff and will form part of the induction process for all staff.

How is content on our tapestry e-profiles managed?

- Staff use tablets to take the photographs for observations which are be uploaded to the journals.
- Each staff member has a secure login which is password protected.

- The tablets are kept in school and may only be taken home by staff members for specific reasons and with the express consent of management.
- Staff are not permitted to download any photographs of the children onto their own devices.
- If staff do work on Tapestry at home, they should be aware of any other people around them and make sure they are not overlooked. They must logout as soon as they have stopped working.
- If any member of staff suspects that their login details have been compromised in any way, they must inform the School Business Manager and new login details will be created.
- The Tapestry on-line Learning Journey system is hosted on secure dedicated servers based in the UK. All data held on our Tapestry account is owned by Child's Play; we are registered controllers of data with the Information Commissioner's Office and are bound by the Data Protection Act.
- Photographs stored on the tablets are deleted on a regular basis by a member of staff.
- Parents logging in to the system can only access their own child's Learning Journey.
- Parents may input new observations and photos and add comments to existing observations. They do not have the necessary permission to edit existing content.
- Parents are asked to sign a consent form giving permission for their child's image to appear within their e-profile.
- When a child leaves the setting, we will email the parents a PDF copy of their child's Learning Journey so they have a lasting record of their child's time at Old Basing.
- Should a child become absent, Tapestry is to be used as the remote learning platform for all year groups.
- Once a child leaves Year 2 the child's information, and their Learning Journey will be permanently deleted from our Tapestry account so no data on that child will remain with us once they have left.

How are E-safety complaints handled?

- Complaints of Internet misuse will be dealt with by the Headteacher.
- Any complaint about staff misuse must be referred to the Headteacher.
- The school will follow the procedures and advice of the local authority.

How is the policy introduced to pupils?

- E-Safety Rules are explained and discussed with all classes by class teachers at a level appropriate to the age of the children. These are reviewed each time pupils have access to the internet.
- E-Safety rules are posted near all computers with Internet access.
- E-Safety will also be addressed through the PSHE and Computing curriculum to inform children of issues that may arise outside of school.
- E-Safety information will be provided on the school website.

How is the policy discussed with staff?

- All staff will be asked to read the School E-Safety Policy and its application and importance will be explained.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- Discretion and professional conduct is essential.
- HSS Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.
- Staff are required to sign an acceptable use policy. If this is breached then the disciplinary processed outlined in this document will be carried out.

The use of social networking sites

- Social networking sites should not be accessed on staff laptops at home or at school. Staff should be extremely vigilant with their privacy settings on any social networking sites and be aware that social networking sites are a public forum.
- Any images that could be considered sensitive should either be removed from social networking sites or be set for viewing by themselves only.
- When writing on social networking sites staff should also consider that these are public forums and should not put into writing anything that they would not want to be publicly shared. Children or parents' names should never be referred to on social networking sites.

- Members of staff should not be 'friends' on social networking sites with parents who have children at the school.
- Staff should not use social networking sites as a media for discussing School care/HSS or school business unless officially endorsed.

How is parents' support enlisted?

- Parents' attention will be drawn to the school's Online Safety Policy in newsletters and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged.
- Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents via the school website and Newsletters.

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for schoolwork only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer or other device when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 4: online safety training needs – self-audit for staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of staff member/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	

ONLINE SAFETY TRAINING NEEDS AUDIT	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5: online safety incident report log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Policy Reviewed: March 2026
By: C.Sciberras (DHT)
Next Review due: September 2026 (Due to changes in guidance from the DfE)