



A Whole School Policy for Online safety

KCSIE 2026 amendments are highlighted in yellow for review and approval.

This policy was approved by the Full Governing Body in September 2025 and has been updated in August 2026 to reflect Keeping Children Safe in Education 2026 (KCSIE 2026), which comes into force on 1 September 2026. The updated policy should be formally approved by the Full Governing Body. To be reviewed September 2027.

To be read in conjunction with our school policy on Child Protection and Safeguarding.

Policy Statement

This Online Safety Policy applies to all members of the school community (including staff, pupils, governors, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

For clarity, the online safety policy uses the following terms unless otherwise stated:

Users - refers to staff, governing body, school volunteers, pupils and any other person working in or on behalf of the school, including contractors.

Parents – any adult with a legal responsibility for the child/young person outside the school e.g. parent, guardian, carer.

School – any school business or activity conducted on or off the school site, e.g. visits, conferences, school trips etc.

Wider school community – pupils, all staff, governing body, parents

KCSIE 2026 online safety framework – The school's approach to online safety is based on four interrelated areas of risk:

Content – exposure to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation and conspiracy theories;

Contact – harmful online interaction with other users or generative AI applications, including grooming and exploitation;

Conduct – online behaviour that increases the likelihood of, or causes, harm, including cyberbullying and the making, sending or receiving of explicit images, including AI-generated images;

Commerce – risks such as online gambling, inappropriate advertising, phishing and financial scams. These risks will inform the school's curriculum, staff training, filtering and monitoring, safeguarding response and parental engagement.

Safeguarding is a serious matter; at Frances Olive Anderson Church of England School we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as online safety, is an area that constantly evolves. In line with KCSIE 2026, the school will review its approach to online safety at least annually, supported by an annual risk assessment that considers and reflects the risks faced by our pupils, and following any significant online safety incident or material change in technology, guidance or risk.



The primary purpose of this policy is twofold:

- To ensure the requirement to empower the whole school community with the knowledge to stay safe and risk free is met.
- To ensure risks are identified, assessed and mitigated (where possible) in order to reduce any foreseeability of harm to the pupil or liability to the school.

This policy is available for anybody to read on the Frances Olive Anderson Church of England Primary School website. Upon review, all members of staff will confirm that they have read and understood the online safety policy and the Staff Acceptable Use Policy Agreement (AUA), which is part of the Staff Code of Conduct. Staff will also receive safeguarding and child protection training, including online safety and their roles and responsibilities in relation to filtering and monitoring, at induction and through regular updates at least annually.

Policy Governance (Roles & Responsibilities)

Governing Body

The governing body is accountable for ensuring that our school has effective policies and procedures in place; as such they will:

- Review this policy annually and in response to any online safety incident to ensure that the policy is up to date, covers all aspects of technology use within the school, to ensure online safety incidents were appropriately dealt with and ensure the policy was effective in managing those incidents.
- Appoint one governor to have overall responsibility for the governance of online safety at the school who will:

Keep up to date with emerging risks and threats through technology use.

Receive regular updates from the Headteacher in regards to training, identified risks and any incidents.

Have online safety as an agenda item at the Full Governing Board meetings.

The Governing Body is responsible for:

- advising on changes to the online safety policy.
- establishing the effectiveness (or not) of online safety training and awareness in the school.
- recommending further initiatives for online safety training and awareness at the school.

Headteacher

Reporting to the governing body, the Headteacher has overall responsibility for online safety within our school. The day-to-day management of this will be delegated to a member of staff, the Online Safety Officer (OSL) as indicated below.

The Headteacher will ensure that:



- Online safety training throughout the school is planned and up to date and appropriate to the recipient, i.e. pupils, all staff, senior leadership team and governing body, parents.
- The designated OSL has had appropriate CPD in order to undertake the day to day duties.
- All online safety incidents are dealt with promptly and appropriately.

The Headteacher Sarah Woolley (who is also DSL) will:

- hold the lead responsibility for online safety, within their safeguarding role.
- Receive relevant and regularly updated training in online safety to enable them to understand the risks associated with online safety and be confident that they have the relevant knowledge and up to date capability required to keep children safe whilst they are online
- meet regularly with the online safety governor to discuss current issues, review (anonymised) incidents and filtering and monitoring reports, and ensure that an effectiveness review of filtering and monitoring is completed at least once every academic year. The review will be carried out by the SLT member responsible for filtering and monitoring, with support from the DSL and IT support, and will include checks that filtering works appropriately on all internet-connected devices in all relevant locations. A record of these checks, findings and resulting actions will be retained.
- attend relevant governing body meetings/groups
- report regularly to the senior leadership team
- be responsible for receiving reports of online safety incidents and handling them, and deciding whether to make a referral by liaising with relevant agencies, ensuring that all incidents are recorded.
- liaise with staff and IT providers on matters of safety and safeguarding and welfare (including online and digital safety)

Online Safety Officer (OSL)

The day-to-day duty of online safety officer is devolved to Stewart Cook with Sarah Woolley as support.

The OSL will:

- Keep up to date with the latest risks to children whilst using technology; familiarize him/herself with the latest research and available resources for school and home use.
- Review this policy regularly and bring any matters to the attention of the Headteacher.
- Advise the Headteacher, governing body on all online safety matters.
- Engage with parents and the school community on online safety matters at school and/or at home.
- Liaise with the local authority, IT technical support and other agencies as required.
- Retain responsibility for the online safety incident log; ensure staff know what to report and ensure the appropriate audit trail.
- Ensure any technical online safety measures in school (e.g. Internet filtering software, behaviour management software) are fit for purpose through liaison with the local authority and/or IT Technical Support.



'Being different, Belonging together'

- Make him/herself aware of any reporting function with technical online safety measures, i.e. internet filtering reporting function; liaise with the Headteacher and responsible governor to decide on what reports may be appropriate for viewing.
- Liaise with the school's Data Protection Officer (DPO).

ICT Technical Support Staff

This policy must be shared with Infotechdirect Ltd who act as our technical staff.

Technical support staff are responsible for ensuring that:

- measures are put in place and periodically reviewed to increase the security and resilience of the school's technical infrastructure, protect personal information, reduce the risk of data breaches and disruption, and mitigate safeguarding risks arising from cyber security incidents.
technical infrastructure and reduce the impact of misuse or a malicious attack.
- they are aware of and follow the school Online Safety Policy to carry out their work effectively in line with school policy
- the school meets (as a minimum) the required online safety technical requirements as identified by the [DfE Meeting Digital and Technology Standards in Schools & Colleges](#) and guidance from local authority
- Anti-virus is fit-for-purpose, up to date and applied to all capable devices.
- Windows (or other operating system) updates are regularly monitored and devices updated as appropriate.
- Any online safety technical solutions such as Internet monitoring and filtering are operating correctly. Filtering and monitoring must be tested on new devices and services before they are made available to pupils and should be checked across all relevant devices, user groups and locations.
- Filtering levels are applied appropriately and according to the age of the user; that categories of use are discussed and agreed with the online safety officer and Headteacher.
- Technical controls support the correct application of passwords to all users regardless of age, in line with school policies.
- If there has been a compromise, a password change will be enforced. The OSL and IT Support will be responsible for ensuring that passwords are changed if required.
- technical controls such as the application of content filtering and monitoring, file permissions and Group Policies are implemented in line with the school's policies and as needs arise in response to requests by the SLT and other staff members. These support the objective of safe and managed control of user access to networks and managed devices. Monitoring should provide information in a format that staff can understand and, where possible, users should be identifiable so that safeguarding concerns can be traced to an individual.
- they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- the use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported to OSL for investigation and action
- the monitoring and filtering software is applied, tested and updated on a regular basis and its implementation is not the sole responsibility of any single person. The school will



'Being different, Belonging together'

maintain a clear division of safeguarding and technical responsibilities between the DSL/SLT and IT support.

Information security and access management – The school treats cyber security as part of its wider safeguarding responsibilities. Appropriate measures will be used to protect personal information, maintain secure access to school systems, reduce the risk of data breaches and disruption, and mitigate safeguarding risks arising from cyber incidents. The school will work towards the DfE Cyber security standards for schools and colleges and review its arrangements through its risk assessment and technology review processes.

All Staff

Staff are to ensure that:

- All details within this policy are understood. If anything is not understood it should be brought to the attention of the Headteacher.
- Any online safety incident or safeguarding concern identified through technology is reported immediately to the OSL/DSL, or in his/her absence to the Headteacher/deputy DSL, in accordance with the school's safeguarding procedures. Staff must not investigate safeguarding concerns themselves. Where an incident involves potentially illegal material, particularly nude or semi-nude images, staff must not view, copy, forward or take possession of the material and must follow the school's safeguarding response.
- The reporting flowcharts contained within this online safety policy are fully understood.

Teaching and teaching support staff are responsible for ensuring that:

- they have an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- they understand that online safety is a core part of safeguarding
- they have read, understood the Staff Code of Conduct which includes acceptable use of the internet
- they immediately report any suspected misuse or problem to the OSL for investigation/action, in line with the school safeguarding procedures
- all digital communications with pupils and parents/carers are on a professional level *and only carried out using official school systems*
- online safety issues are embedded in all aspects of the curriculum and other activities
- ensure pupils understand and follow the Online Safety Policy and acceptable use agreements, have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they supervise and monitor the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- in lessons where internet use is pre-planned pupils are guided to sites checked as suitable for their use *and that processes are in place for dealing with any unsuitable material that is found in internet searches*
- where lessons take place using live-streaming or video-conferencing, there is regard to national safeguarding guidance and local safeguarding policies



'Being different, Belonging together'

- there is a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, hatred etc
- they model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Pupils

All pupils are responsible for using the school digital technology systems in accordance with the pupil acceptable use agreement and Online Safety Policy.

Pupils should

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- know what to do if they or someone they know feels vulnerable when using online technology
- understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents and Carers

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

The school will take every opportunity to help parents and carers understand these issues through:

- publishing the school Online Safety Policy on the school website
- providing them with a copy of the pupils' acceptable use agreement
- publish information about appropriate use of social media relating to posts concerning the school.
- seeking their permissions concerning digital images, cloud services etc (see parent/carers AUA in the appendix)
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents and carers will be encouraged to support the school in:

- reinforcing the online safety messages provided to pupils in school.
- the safe and responsible use of their children's personal devices by understanding that the devices.

The School Online Safety Policy:

- sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication
- allocates responsibilities for the delivery of the policy



'Being different, Belonging together'

- is regularly reviewed in a collaborative manner, taking account of online safety incidents, the annual online safety risk assessment, the effectiveness of filtering and monitoring, and changes/trends in technology and related behaviours
- establishes guidance for staff in how they should use digital technologies responsibly, protecting themselves and the school and how they should use this understanding to help safeguard pupils in the digital world
- describes how the school will help prepare pupils to be safe and responsible users of online technologies
- establishes clear procedures to identify, report, respond to and record the misuse of digital technologies and online safety incidents, including external support mechanisms
- is supplemented by a series of related acceptable use agreements
- is made available to staff at induction, INSET training, staff notice board
- is published on the school website

Generative Artificial Intelligence (AI) – Where generative AI tools are used by staff or pupils, they must be appropriately risk assessed and approved for educational use. The school will consider safeguarding, privacy/data protection, intellectual property, accuracy, bias and age-appropriateness. Where pupils use AI, the school will provide age-appropriate teaching about safe and responsible use, including the risks of harmful or misleading content, deepfakes, image manipulation, privacy and over-reliance on AI.

Technology

Frances Olive Anderson Church of England School uses a range of devices including PC's, laptops, iPads and tablets. In order to safeguard staff and pupils and in order to prevent loss of personal data we employ the following assistive technology:

Internet Filtering – Infotechdirect uses Fortinet software through an onsite Fortigate Appliance that restricts access to malicious websites that may pose a risk to users and equipment. It also restricts access to inappropriate web content; appropriate and inappropriate content is determined by the age and needs of the user and will be reviewed in line with this policy, the school's risk assessment, changes in safeguarding risks or in response to an incident, whichever is sooner. In line with KCSIE 2026, the school will ensure that filtering and monitoring are appropriate, effective and reviewed at least annually, including checks on all internet-connected devices and relevant locations. The school will avoid over-blocking where this would unreasonably restrict teaching and learning, while maintaining appropriate safeguards.

Email Filtering – Office 365 Spam Protection software reduces the likelihood of infected emails being sent from the school, or received by the school. Infected is defined as: an email that contains a virus or script (i.e. malware) that could be damaging or destructive to data; spam email such as a phishing message.

Encryption – The school laptops are encrypted using 'Bitlocker'. All the data on the PC's on site is stored on the school's server. No data is to leave the school on an un-encrypted device; all devices that are kept on school property and which may contain personal data are encrypted. Any breach (i.e. loss/theft of device such as laptop) is to be brought to the attention of the Headteacher immediately. The Headteacher will liaise with the local authority to ascertain whether a report needs to be made to the Information Commissioner's Office (Note: Encryption does not mean password protected.)



Passwords – staff passwords must be strong, unique and kept confidential. They should meet the school's minimum password requirements and use multi-factor authentication where this is available and appropriate.

Children should log in with their own unique username and password. Pupil credentials should be age-appropriate, unique and kept confidential; predictable or easily guessed credentials should be avoided.

The network is not currently segmented; however, file permissions are applied to prevent children accessing areas that are restricted to staff.

Children should be educated to keep their passwords secret and not share them with other children.

Anti-Virus – All capable devices will have Fortclient. This software updates daily for new virus definitions. IT Support will be responsible for ensuring this task is carried out, and will report to the Headteacher if there are any concerns. All USB peripherals such as keydrives (if you allow them) are to be scanned for viruses before use.

Safe Use

Internet – Use of the Internet in school is a privilege, not a right. Internet use will be granted: to staff upon signing this online safety and the staff Acceptable Use Policy; pupils upon signing and returning their acceptance of the Acceptable Use Policy that is incorporated in the 'School Booklet'.

Email – All staff are reminded that emails are subject to Freedom of Information requests, and as such the email service is to be used for professional work-based emails only. Emails of a personal nature are not permitted. Similarly use of personal email addresses for work purposes is not permitted.

Photos and videos – Digital media such as photos and videos are covered in the schools' Photography and Mobile Phone Policy and is re-iterated here for clarity. All parents must sign a photo/video release slip at the beginning of each academic year; non-return of the permission slip will not be assumed as acceptance.

Social Networking – there are many social networking services available; Frances Olive Anderson Church of England Primary School may use approved social media services to engage with parents and the wider school community. Any service used by the school must be appropriately risk assessed and approved before use. Staff must not use personal social media accounts to communicate directly with pupils or parents/carers on behalf of the school.

- Facebook – for Snippets and other information flyers.

A broadcast service is a one-way communication method in order to share school information with the wider school community. No persons will be "followed" or "friended" on these services and as such no two-way communication will take place.

In addition, the following is to be strictly adhered to:



'Being different, Belonging together'

- Permission slips (included in the Appendices and School Booklet) must be consulted before any image or video of any child is uploaded.
- There is to be no identification of pupils at all.
- All posted data must conform to copyright law; images, videos and other resources that are not originated by the school are not allowed unless the owner's permission has been granted or there is a license which allows for such use (i.e. creative commons).

Notice and take down policy – should it come to the schools attention that there is a resource which has been inadvertently uploaded, and the school does not have copyright permission to use that resource, it will be removed within one working day.

Child-on-child online abuse –

The school recognises that children can abuse other children online. This may include cyberbullying, abusive or harassing messages, misogynistic (showing a hatred of, contempt for, or prejudice against women and girls) or misandrist (a person who holds a deep dislike, contempt, or hatred for men or boys) abuse, harmful sexual behaviour, sexual harassment, and the consensual or non-consensual making or sharing of nude or semi-nude images, including images generated or altered using AI. All such concerns will be taken seriously and managed through the school's safeguarding procedures.

Incidents –

Any online safety incident is to be brought to the immediate attention of the OSL/DSL, or in his/her absence the Headteacher/deputy DSL. The OSL/DSL will assist in taking the appropriate safeguarding action and recording the incident according to school procedure. Online incidents involving child-on-child abuse, cyberbullying, sexual harassment, sexual violence, or the making/sharing of nude or semi-nude images (including AI-generated images) require a safeguarding response. Staff must not investigate potentially illegal images or material themselves; evidence should be preserved safely and advice sought from the DSL and, where appropriate, the police or other relevant safeguarding agency.

Training and Curriculum –

It is important that the wider school community is sufficiently empowered with the knowledge to stay as safe as possible whilst using digital technology; this includes updated awareness of new and emerging issues. Online safety education will reflect the four areas of online risk identified in KCSIE 2026: content, contact, conduct and commerce. It will also address age-appropriate issues including cyberbullying, misinformation and disinformation, online scams, harmful content, grooming, image sharing, pornography, deepfakes and other AI-generated content, and how and where to seek help. Staff training will include online safety and the expectations, roles and responsibilities relating to filtering and monitoring at induction and through regular updates at least annually.

Online safety for pupils is embedded into the curriculum; whenever ICT is used in the school, staff will ensure that there are positive messages about the safe use of technology and risks as part of the pupil's learning. Each year as part of our Keeping Children Safe in Education and Safeguarding training teaching online safety in school is covered with reference to <https://www.gov.uk/government/publications/teaching-onlineonline-safety-in-schools>

As well as the programme of training we will establish further training or lessons as necessary in response to any incidents.

The OSL is responsible for recommending a programme of training and awareness for the school year to the Headteacher and responsible Governor for consideration and planning. Should any



‘Being different, Belonging together’

member of staff feel they have had inadequate or insufficient training generally or in any particular area this must be brought to the attention of the Headteacher for further CPD.

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown below.

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and pupils or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. *Personal e-mail addresses, text messaging or social media must not be used for these communications.*
- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to the Headteacher or OSL – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum for all year groups matched against a nationally agreed framework (Teach Computing Curriculum) and regularly taught in a variety of contexts.
- Lessons are matched to need; are age-related and build on prior learning
- Lessons are context-relevant with agreed objectives leading to clear and evidenced outcomes
- Pupil need and progress are addressed through effective planning and assessment. Digital competency is planned and effectively threaded through the appropriate digital pillars in other curriculum areas e.g. PHSE; SRE; Literacy etc
- it incorporates/makes use of relevant national initiatives and opportunities e.g. [Safer Internet Day](#) and [Anti-bullying week](#)
- the programme will be accessible to pupils at different ages and abilities such as those with additional learning needs or those with English as an additional language.
- vulnerability is actively addressed as part of a personalised online safety curriculum e.g., for victims of abuse and SEND.
- Pupils should be helped to understand the need for the pupil acceptable use agreement and encouraged to adopt safe and responsible use both within and outside school. Acceptable use is reinforced across the curriculum, with opportunities to discuss how to act within moral and legal boundaries online, including the risks associated with cyberbullying, harmful online content, misinformation and disinformation, scams, grooming, sharing images, AI-generated content and deepfakes. Lessons should be age-appropriate and responsive to the needs and vulnerabilities of individual pupils.
- staff should act as good role models in their use of digital technologies the internet and mobile devices



'Being different, Belonging together'

- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- where pupils are allowed to freely search the internet, staff should be vigilant in supervising the pupils and monitoring the content of the websites the young people visit
- it is accepted that from time to time, for good educational reasons, pupils may need to research topics, (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff should be able to request the temporary removal of those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need
- the online safety education programme should be relevant and up to date to ensure the quality of learning and outcomes.

Contribution of Pupils

The school acknowledges, learns from, and uses the skills and knowledge of pupils in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the school community and how this contributes positively to the personal development of young people. Their contribution is recognised through:

- mechanisms to canvass pupil feedback and opinion
- appointment of digital leaders/anti-bullying ambassadors/peer mentors
- pupils contribute to the online safety education programme e.g. peer education, online safety campaigns
- contributing to online safety events with the wider school community e.g. parents' evenings, family learning programmes etc.

Staff/volunteers

All staff will receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- will be an integral part of the school's annual safeguarding and data protection training for all staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- all new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use agreements. It includes explicit reference to classroom management, professional conduct, online reputation and the need to model positive online behaviours.
- the Online Safety Lead and Designated Safeguarding Lead (or other nominated person) will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- this Online Safety Policy and its updates will be presented to and discussed by staff in staff/team meetings/INSET days
- the Designated Safeguarding Lead/Online Safety Lead (or other nominated person) will provide advice/guidance/training to individuals as required.



Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any sub-committee/group involved in technology/online safety/health and safety/safeguarding. This may be offered in several ways such as:

- attendance at training provided by the local authority or other relevant organization.
- participation in school training / information sessions for staff or parents.

A higher level of training will be made available to (at least) the Online Safety Governor. This will include:

- Cyber-security training (at least at a basic level)
- Training to allow the governor to understand the school's filtering and monitoring provision, in order that they can participate in the required checks and review.

Families

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will seek to provide information and awareness to parents and carers through:

- regular communication, awareness-raising and engagement on online safety issues, curriculum activities and reporting routes
- regular opportunities for engagement with parents/carers on online safety issues through awareness workshops / parent/carers evenings etc
- the pupils – who are encouraged to pass on to parents the online safety messages they have learned in lessons and by pupils leading sessions at parent/carers evenings.
- letters, newsletters, website,
- high profile events / campaigns e.g. [Safer Internet Day](#)
- reference to the relevant web sites/publications, e.g. [SWGfL](#); www.saferinternet.org.uk/; www.childnet.com/parents-and-carers (see Appendix for further links/resources).
- Sharing good practice with other schools in clusters and or the local authority.

Parents and carers will be informed, as appropriate, about the school's filtering and monitoring arrangements and about online activities pupils may be asked to undertake, including the websites, platforms or services they may be expected to access and who they may interact with online.

Acceptable Use Policy Agreements (AUA)

The Online Safety Policy and Acceptable Use Policy Agreements define acceptable use at the school.

AUA's will be communicated/re-enforced through:

- School Booklet
- staff induction and Code of Conduct
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website



'Being different, Belonging together'

Staff and Volunteer Acceptable Use Agreement – this is part of the Staff Code of Conduct

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement – is contained within the Staff Code of Conduct

I have read and understand the above and agree to use the school digital technology .



Pupil Acceptable Use Agreement – KS2

This Acceptable Use Agreement (AUA) is intended:

- to ensure that pupils will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help pupils understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

Acceptable Use Agreement

When I use devices I must behave responsibly to help keep me and other users safe online and to look after the devices.

For my own personal safety:

- I understand that what I do online will be supervised and monitored and that I may not be allowed to use devices in school unless I follow these rules and use them responsibly.
- I will only visit internet sites that adults have told me are safe to visit.
- I will keep my username and password safe and secure and not share it with anyone else.
- I will be aware of “stranger danger” when I am online.
- I will not share personal information about myself or others when online.
- I will immediately tell an adult if I see anything that makes me feel uncomfortable when I see it online.

I will look after the devices I use, so that the school and everyone there can be safe:

- I will handle all the devices carefully and only use them if I have permission.
- I will not try to alter the settings on any devices or try to install any software or programmes.
- I will tell an adult if a device is damaged or if anything else goes wrong.
- I will only use the devices to do things that I am allowed to do.
- I will think about how my behaviour online might affect other people:
- When online, I will act as I expect others to act toward me.
- I will not copy anyone else's work or files without their permission.
- I will be polite and responsible when I communicate with others, and I appreciate that others may have different opinions to me.
- I will not take or share images of anyone without their permission.

I know that there are other rules that I need to follow:



'Being different, Belonging together'

- I will not use my own personal devices, including mobile phones or smart watches, in school. I will place my device in the school's 'phone box' stored in the school office during the school day. I understand that the school is a mobile-phone-free environment by default and that exceptions are only permitted where agreed by the school.
- I will only use social media sites with permission and at the times that are allowed.
- Where work is protected by copyright, I will not try to download copies (including music and videos).
- When I am using the internet to find information, I should take care to check that the information is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.
- I should have permission if I use the original work of others in my own work.

I understand that I am responsible for my actions, both in and out of school:

- I know that I am expected to follow these rules in school and that I should behave in the same way when out of school as well.
- I understand that if I do not follow these rules, I may be subject to disciplinary action. This could include loss of access to the school network/internet, parents/carers contacted and in the event of illegal activities involvement of the police.

Pupil Acceptable Use Agreement Form

Please complete the sections below to show that you have read, understood and agree to the rules included in the acceptable use agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the school systems and devices (both in and out of school)
- I do not use my own devices in the school e.g. mobile phones, gaming devices USB devices, cameras etc.
- I am out of school and involved in any online behaviour that might affect the school or other members of the school.

Signed (child): Year:.....
Signed (Parent): Date:



Pupil Acceptable Use Agreement (KS1)

This Acceptable Use Agreement (AUA) is intended:

- to ensure that pupils will have good access to devices and online content, be responsible users and stay safe while using digital technologies for educational, personal and recreational use
- to help pupils understand good online behaviours that they can use in school, but also outside school
- to protect school devices and networks from accidental or deliberate misuse that could put the security of the systems and users at risk.

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers/tablets.
- I will only use activities that a teacher or suitable adult has told or allowed me to use.
- I will take care of computers/tablets and other equipment.
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.
- I will tell a teacher or suitable adult if I see something that upsets me on the screen.
- I know that if I break the rules, I might not be allowed to use a computer/tablet.

Signed (child):

Signed (parent):Date:



Parent/Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open new opportunities for everyone. They can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This acceptable use policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of online safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that pupil have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users. A copy of the pupil acceptable use agreement is attached to this permission form, so that parents/carers will be aware of the school expectations of the young people in their care.

As part of our desire to ensure all children are safe when using social media and are free from bullying behaviour, it is expected that all parents watch the following clip from Lincolnshire's Stay Safe Partnership: <https://youtu.be/Akl9CgpP9t8?si=fva0TnHhuGCY-73J>

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent/Carers Name:

Pupil Name:

As the parent/carers of the above pupil, I give permission for my son/daughter to have access to the digital technologies at school.

KS2

I know that my son/daughter has signed an acceptable use agreement and has received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Reception/KS1

I understand that the school has discussed the acceptable use agreement with my son/daughter and that they have received, or will receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including appropriate filtering and monitoring systems, to help ensure that young people are safe when they use the internet and school systems. I understand that the school will review the effectiveness of its filtering and monitoring at least annually and that I can ask the school for information about the systems used to filter and monitor online activity.



'Being different, Belonging together'

I understand that my son's/daughter's activity on the systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the acceptable use agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's online safety.

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Pupils and members of staff may use digital devices to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media. Where an image is publicly shared by any means, only your child's first name will be used and only with your permission

The school will comply with applicable data protection laws, including the UK GDPR, the Data Protection Act 2018 and the Data (Use and Access) Act 2025, and will request parent/carers permission where required before taking images of members of the school community. We will ensure that images are used and published in accordance with the school's data protection, photography and safeguarding arrangements.

Parents/carers are welcome to take videos and digital images of their children at school events for their own personal use where permitted by the school. To respect privacy and safeguarding, parents/carers should only take images of their own children and should not publish or make publicly available images containing other pupils, unless they have the appropriate permission. The school may restrict photography or recording at particular events where safeguarding, privacy or other legitimate concerns require this.

Parents/carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents/carers to agree.

Digital/Video Images Permission Form

Parent/Carers Name: **Pupil Name:**

As the parent/carers of the above pupil, I agree to the school taking digital/video images of my child/children.	Yes/No
I agree to these images being used:	
to support learning activities.	Yes/No
in publicity that reasonably celebrates success and promotes the work of the school.	Yes/No



'Being different, Belonging together'

images may be published on the school's website and Facebook page, in the school's newsletter Snippets and via the schools communication software Parent Hub	Yes/No
I agree that if I take digital or video images at, or of school events which include images of children, that they will not include images of other children. I will abide by these guidelines in my use of these images.	Yes/No

Signed:
Date:

Use of Cloud Systems Permission Form

The school uses Seesaw for Y1 – Y6 and Tapestry for Reception pupils and staff. This permission form describes the tools and pupil responsibilities for using these services. Using Seesaw and Tapestry will enable your child to collaboratively create, edit and share files and websites for school related projects and communicate with members of staff. These services are entirely online and available 24/7 from any internet-connected device. The school believes that use of the tools significantly adds to your child's educational experience.

Do you consent to your child to having access to this service? Yes/No

Pupil Name: Parent/Carers Name:
Signed Date:

The data shared with the service provider is: Child's name and Class – Seesaw. Child's name, date of birth and parent/carers email address -Tapestry.

This form will be stored with your child's school information in a locked cupboard. It will only be accessed by the school's teaching and office staff and if necessary the school's online safety governor. It will be renewed annually. It will be securely destroyed when your child leaves this school.



Reporting Log						
Date	Time	Incident	Action Taken		Incident Reported By	Signature
			What?	By Whom?		



'Being different, Belonging together'

--	--	--	--	--	--	--



'Being different, Belonging together'
Online Safety Incident

