



Risby CEVC Primary School

Online Safety Policy

Prepared by:	Lucy Smith
Approved by:	Chair of Governors
Signature of Chair of Governors:	
Date approved:	September 2026
Review Date:	September 2027

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

Legislation and guidance

This Online Safety Policy outlines the commitment of the school to safeguard members of our school community online in accordance with statutory guidance and best practice.

The school provides appropriate privacy notices to staff, governors, volunteers, parents/carers and pupils, explaining how personal information is collected, used, stored and protected. Pupil privacy information is provided in an age-appropriate and accessible form. Relevant privacy information is also published on the school website. Privacy notices are maintained as separate controlled documents and are reviewed and updated as required.

It reflects relevant legislation, including the Education Act 1996 (as amended), the Education and Inspections Act 2006, the Equality Act 2010, the Education Act 2011, the UK GDPR and Data Protection Act 2018 as amended by the Data (Use and Access) Act 2025, and the Children's Wellbeing and Schools Act 2026. Any searching, examination or deletion of data on a pupil's device will be undertaken only in accordance with current statutory guidance and the school's Behaviour Policy.

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

This Online Safety Policy applies to all members of the school community (including staff, learners, 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).

The four areas of online safety risk

KCSIE identifies four broad areas of online safety risk. Risby CEVC Primary School uses these areas to inform its curriculum, safeguarding response, filtering and monitoring arrangements and staff training:

- Content - being exposed to illegal, inappropriate or harmful content, including pornography, misogyny, self-harm or suicide content, misinformation and disinformation, racist or discriminatory content, and content that promotes extremism.

- Contact - being subjected to harmful online interaction with other users, including peer pressure, commercial advertising, adults posing as children or young adults, grooming, exploitation and other harmful contact.
- Conduct - personal online behaviour that increases the likelihood of, or causes, harm, including making, sending or receiving explicit images, online bullying and harmful or inappropriate use of AI-generated or manipulated content.
- Commerce - risks such as online gambling, inappropriate advertising, phishing, scams and other financial harms.

Risby CEVC Primary School will respond to online safety incidents in accordance with this policy and the school's safeguarding, behaviour and anti-bullying procedures. Where an incident outside school has a safeguarding impact on a pupil or affects the orderly running of the school, the school will respond appropriately and, where appropriate, inform parents/carers and relevant agencies.

Roles and responsibilities

To ensure the online safeguarding of members of our school community it is important that all members of that community work together to develop safe and responsible online behaviours, learning from each other and from good practice elsewhere, reporting inappropriate online behaviours, concerns, and misuse as soon as these become apparent. While this will be a team effort, the following sections outline the online safety roles and responsibilities of individuals and groups within the school.

The governing body

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

Governors are responsible for approving this Online Safety Policy and for reviewing its effectiveness, including the effectiveness of the school's filtering and monitoring arrangements.

The governing body will receive appropriate information about online safety, including anonymised safeguarding themes, filtering and monitoring assurance, staff training and curriculum provision. Governors will provide appropriate challenge and support to the Headteacher and DSL.

All governors will:

- Ensure that 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 2)

- Sign the school's Acceptable Use Agreement and receive/acknowledge the relevant Privacy Notice(s); the school retains appropriate records
- Support the school in encouraging parents/carers and the wider community to become engaged in online safety activities.

The Safeguarding Governor, Laura Marshall, provides particular oversight of safeguarding and online safety on behalf of the governing body. This includes:

- regular safeguarding monitoring with the Headteacher/DSL/Online Safety Lead, Mrs Lucy Smith
- regularly receiving (collated and anonymised) reports of online safety incidents
- checking that provision outlined in this policy is taking place as intended, including online safety education, staff training, the annual review of filtering and monitoring arrangements, and reporting to relevant governors' meetings

The headteacher

The headteacher will act as the Online Safety Lead and is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. They will do this by:

- ensuring the safety (including online safety) of members of the school community and fostering a culture of safeguarding
- being aware (alongside the Deputy Headteacher and DSL/ADSLs) of the procedures to be followed in the event of a serious online safety concern or an allegation or low-level concern involving a member of staff
- being responsible for ensuring that technical staff, and other relevant staff carry out their responsibilities effectively and receive suitable training to enable them to carry out their roles and train other colleagues, as relevant.
- ensuring that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- have a leading role in establishing and reviewing the school online safety policies/documents
- promote an awareness of and commitment to online safety education / awareness raising across the school and beyond
- liaise with curriculum leaders to ensure that the online safety curriculum is planned, mapped, embedded and evaluated
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place and the need to immediately report those incidents

- receive reports of online safety incidents and follow up actions from these
- provide (or identify sources of) training and advice for staff/governors/parents/carers/learners
- liaise with JC Comtech and other relevant external services, as required
- meet with the Safeguarding Governor, Laura Marshall, as part of safeguarding monitoring to discuss current issues, review anonymised incidents and provide assurance about filtering and monitoring arrangements
- report regularly to governors

The Headteacher is also responsible for:

- Ensuring that appropriate filtering and monitoring systems are in place and are suitable for the school's age range, curriculum, safeguarding risks and use of technology, without unreasonably restricting teaching and learning
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Ensuring that the effectiveness of filtering and monitoring arrangements is reviewed at least annually, and sooner where there is a significant change to systems, risk or provision
- Ensuring that filtering or monitoring concerns, alerts and breaches are acted upon promptly, with safeguarding concerns referred to the DSL or ADSL and technical faults escalated to JC Comtech
- Ensuring that any online safety incidents are logged (on MyConcern) and dealt with appropriately in line with this policy
- Ensuring 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.

The other designated safeguarding staff

The safeguarding team comprises Mrs Lucy Smith (Headteacher, DSL and Online Safety Lead), Adele Jones (ADSL) and Louise Filby (ADSL). Full safeguarding arrangements are set out in the school's Safeguarding and Child Protection Policy.

Safeguarding staff take responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, JC Comtech and other staff, as necessary, to address online safety issues or incidents

- Ensuring that any online safety incidents are logged (on MyConcern) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school anti-bullying policy
- Ensuring staff receive online safety training at induction and at least annual safeguarding updates, with additional updates where new risks or technologies emerge
- 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

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
- understanding that online safety is a core part of safeguarding
- having an awareness of current online safety matters/trends and of the current school Online Safety Policy and practices
- implementing this policy consistently
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendix 1)
- signing the school's Acceptable Use Agreement and receiving/acknowledging the relevant Privacy Notice(s); the school retains appropriate records
- working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- ensuring that all digital communications with learners and parents/carers should be on a professional level and only carried out using official school systems
- ensuring that online safety issues are embedded in all aspects of the curriculum and other activities
- ensure learners 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

- supervising and monitoring the use of digital technologies, mobile devices, cameras, etc., in lessons and other school activities (where allowed) and implement current policies regarding these devices
- ensuring that learners 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
- ensuring that where lessons take place using live-streaming or video-conferencing, staff must have full regard to national safeguarding guidance and local safeguarding policies
- responding to online bullying, sexual harassment, discrimination, hateful content and other harmful online behaviour as safeguarding and/or behaviour concerns, as appropriate
- modelling safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media.

Curriculum Leads will work with the Online Safety Lead to develop a planned and coordinated online safety education programme

This will be provided through:

- PSHE and RSE programmes
- mapped cross-curricular sessions
- assemblies and pastoral programmes
- and through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.

The school does not operate official social-media accounts. The school website is used to publish policies and relevant information for parents/carers.

Reception/EYFS uses Tapestry to record and share children's learning. Authorised Reception staff and the child's parents/carers may access the child's learning record, and parents/carers may contribute observations. Users must respect the confidentiality of other children and families and must not copy or publicly share images or information about other children.

Risby CEVC Primary School uses ClassDojo, Arbor and school email as approved channels for communication with parents/carers. Staff must use approved school systems for professional communication and must not use personal social-media accounts or personal messaging accounts to communicate with pupils or families about school matters.

Approved school platforms and communication

Parents

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 parents/carers with the pupil acceptable use agreement and explaining the school's expectations for safe and responsible technology use
- publish information about appropriate use of social media, games and other online content
- explaining the school's arrangements for digital images, approved cloud services and other online services where consent or information is required
- parents'/carers' evenings, newsletters, website, social media and information about national/local online safety campaigns and literature.

Parents are expected to:

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

Parents can seek further guidance from trusted sources including the UK Safer Internet Centre, Childnet, Internet Matters and CEOP Education. The school will signpost current resources through its website, newsletters and other communications rather than relying on fixed links that may become outdated.

Visitors and members of the community

Visitors and members of the community who need internet access may request access to the school's separate guest Wi-Fi network. Guest Wi-Fi credentials are not openly available and are provided only when required. Visitors, contractors and external providers must follow the school's acceptable-use and safeguarding expectations. External providers do not normally use school iPads, laptops or other IT systems; any exceptional access must be specifically authorised and appropriately supervised or controlled.

Learners

- are responsible for using the school digital technology systems in accordance with the learner acceptable use agreement and Online Safety Policy
- should understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should know what to do if they or someone they know feels vulnerable when using online technology
- should 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.

Educating pupils about online safety

Online safety is taught from Reception onwards through age-appropriate provision, the Computing curriculum and SCARF PSHE. Teaching is revisited across the school and adapted to pupils' age, development and needs.

In Reception/EYFS, children are introduced to age-appropriate online-safety messages, including asking a trusted adult for help, using devices with adult guidance, treating others kindly and understanding that not everything seen or heard on a screen is reliable or suitable.

In Key Stage 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

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

The safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies, curriculum opportunities and national initiatives such as Safer Internet Day and Anti-Bullying Week to reinforce age-appropriate online safety messages. External speakers may be used where they add value and have been appropriately checked and briefed.

Pupils are encouraged to tell any trusted adult in school if something online worries, frightens, confuses or upsets them, or if they are concerned about another child. This may be their class teacher, another member of staff, Mrs Lucy Smith (DSL), Adele Jones (ADSL) or Louise Filby (ADSL). The adult will listen, take the concern seriously and pass safeguarding information to the DSL/ADSL as required. If a concern involves an adult working at the school, staff will follow the school's procedures for concerns or allegations about adults.

How pupils can report an online-safety concern

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. This policy will also be shared with parents.

Online safety information may also be shared at parent meetings and through school communications. Parents/carers should raise concerns with the class teacher, DSL/ADSL or Headteacher as appropriate to the nature and urgency of the concern.

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

Generative artificial intelligence (AI) and emerging technologies

Pupils do not currently use generative AI tools in school. Pupils must not use generative AI through school accounts, devices or systems unless the school has expressly authorised a future supervised educational activity and has considered age restrictions, safeguarding, filtering and monitoring, data protection and the educational purpose. Age-appropriate teaching will help pupils understand AI-generated and manipulated content, misinformation and the importance of seeking help when content is worrying or harmful.

Staff may use generative AI to support planning and the creation/adaptation of resources. Microsoft Copilot is available to staff through the school's Microsoft 365 environment and is an approved tool for these purposes. Staff remain professionally responsible for checking AI-generated output for accuracy, bias, copyright, safeguarding, age-appropriateness and suitability before use. Staff must follow the school's data-protection requirements and must not place safeguarding information, special-category data or confidential/personal information into AI services unless that specific processing has been approved by the school.

The school recognises that generative AI can support education and administration but may also create safeguarding, accuracy, copyright, bias and data-protection risks. Any use must be age-appropriate, lawful, transparent and consistent with school policies and DfE guidance.

Digital images, video and school events

Parents/carers may take photographs or video at school performances, assemblies, sports days and similar events where the school permits this. They will be reminded that images or recordings containing other children must not be posted publicly or shared on social media. Safeguarding restrictions or specific circumstances may mean photography or recording is not permitted at a particular event.

The school obtains and records parent/carer consent or preferences for the use of pupil photographs and video, including use in Tapestry, on the school website, in newsletters and on displays. Staff must check the relevant permissions before images are used or published.

Staff must report concerns immediately to the DSL/ADSL in accordance with the Safeguarding and Child Protection Policy. The school will take a child-centred approach, consider the needs and safety of all children involved, preserve evidence appropriately, involve parents/carers where appropriate and seek advice or refer to external agencies when required.

Online child-on-child abuse and harmful sexual behaviour

Online harm between children can include bullying, harassment, sexual harassment, coercion, threats, impersonation, exclusion, abuse in group chats or games, non-consensual sharing of images, and the creation or sharing of manipulated or AI-generated sexualised content. Such behaviour may occur wholly online or form part of abuse occurring offline.

Cyber-bullying

Definition

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the anti-bullying policy).

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.

Teaching staff will address online bullying through age-appropriate class discussion, PSHE/RSE, Computing, assemblies and other curriculum opportunities, rather than relying on a single lesson or event.

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 and governors receive appropriate online safety training as part of safeguarding training and updates.

The school will share current guidance with parents/carers to help them recognise online bullying, report concerns and support children who may be affected.

In relation to a specific incident of online bullying, the school will follow its Positive Behaviour Policy, Anti-Bullying Policy and safeguarding procedures as appropriate. Where illegal, inappropriate or harmful material has been shared, the school will take reasonable steps to safeguard pupils, preserve relevant evidence and contain further sharing.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so. 6

Examining electronic devices

Authorised school staff may search pupils and examine or confiscate electronic devices only in accordance with current DfE statutory guidance on searching, screening and confiscation and the school's Behaviour Policy. Where a device may contain evidence of a safeguarding concern or criminal offence, staff will seek advice from the DSL before viewing, copying or deleting material unless immediate action is necessary to protect a child.

Particular care will be taken where an incident may involve nude or semi-nude images, sexual content, child sexual abuse material, threats, exploitation or other potentially illegal material. Staff must not intentionally view, copy, print, forward or save such material unless specifically required and authorised as part of an appropriate safeguarding or law-enforcement response. The DSL will follow current safeguarding guidance and contact the police or other agencies where required.

Any searching of pupils will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

Acceptable use of the internet in school

All pupils, parents, 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 and 2). All staff and governors sign and comply with the school's Acceptable Use Agreement and are provided with the relevant Privacy Notice(s), acknowledging receipt where required. The school retains appropriate records of signed Acceptable Use Agreements and privacy information provided. 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.

The school uses filtering and monitoring arrangements to help safeguard users of school systems and devices. Monitoring is proportionate, transparent and restricted to authorised staff. Safeguarding alerts or concerns are passed promptly to the DSL/ADSL, while technical faults are escalated to JC Comtech. The school's privacy information explains relevant monitoring of personal data.

Access to monitoring reports and alerts will be limited to authorised staff who have appropriate training. The school will ensure that alerts can be linked to identifiable users where reasonably possible, that safeguarding concerns are escalated to the DSL/ADSL, and that decisions and actions are recorded. Before introducing a new filtering or monitoring system, or making a significant change, the school will consider data-protection requirements including whether a Data Protection Impact Assessment is required.

Filtering and monitoring are part of the school's safeguarding arrangements and do not replace effective supervision, education or professional curiosity. The Headteacher/Online Safety Lead, DSL and governing body will understand the school's arrangements and their limitations. The school will work with its JC Comtech to ensure that systems operate as intended on relevant school networks and devices, including where school-managed devices are used away from the site where technically applicable.

Filtering and monitoring

JC Comtech provides Risby CEVC Primary School's internet filtering and monitoring provision. Filtering and monitoring form part of the school's safeguarding arrangements and do not replace effective supervision, online-safety education or professional curiosity. Pupils use individual usernames and passwords, including school email accounts for curriculum purposes and saving work, so that activity can be associated with the appropriate user where reasonably possible.

Mrs Lucy Smith, as DSL and Online Safety Lead, receives a daily filtering and monitoring report from JC Comtech. She reviews the report and investigates concerning activity, speaking with the pupil or member of staff as appropriate. Where an item constitutes a safeguarding

concern, the concern, action and outcome are recorded on MyConcern. High-risk concerns or alerts are acted upon promptly in accordance with the school's safeguarding procedures.

The school's filtering and monitoring arrangements are formally reviewed at least annually by the Headteacher/DSL/Online Safety Lead with JC Comtech and governor oversight. An additional review will take place following a significant safeguarding incident, a substantial change to technology or systems, or where evidence indicates that current arrangements may no longer be appropriate. The review and any resulting actions will be recorded.

Governors monitor the effectiveness of the school's filtering and monitoring systems as part of their safeguarding oversight. Laura Marshall, Safeguarding Governor, has particular oversight through safeguarding monitoring.

Filtering and monitoring are configured with regard to the age and needs of pupils, including pupils with SEND, and should block harmful and inappropriate content without unreasonably restricting teaching and learning. Staff remain responsible for active supervision of pupils using technology.

Pupil smartwatches are not permitted in school.

Pupils have individual school usernames and passwords, including school email accounts used for curriculum purposes and saving work. Pupils must keep credentials private, use only their own account and log out when appropriate. School accounts and activity are subject to the school's filtering and monitoring arrangements.

Pupils use school iPads and laptops for curriculum purposes. School-owned devices are not normally taken home by pupils and may only be taken off site in exceptional circumstances with school authorisation. Where this occurs, the school's safeguarding, filtering/monitoring, data-protection and acceptable-use expectations continue to apply.

School devices, pupil accounts and wearable technology

Pupils using mobile devices in school

Year 5 and Year 6 pupils may bring a mobile phone or other personal interactive communication device to school only where this is needed for travel to or from school and the school has written parental/carer permission. On arrival, the device must be switched off and handed to the school office to be signed in and stored securely. It is returned at the end of the school day. Pupils must not have access to or use personal mobile phones or other personal interactive communication devices during the school day, including lessons, breaktimes and lunchtime. This arrangement supports the school's mobile-phone-free school day while allowing devices to be available for journeys to and from school.

- Pupils must not use personal mobile phones or other personal interactive communication devices during the school day.

- The same expectation applies during school-organised clubs and activities unless the Headteacher has authorised a specific exception or reasonable adjustment.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendix 1).

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

Staff must not use personal social-media accounts, personal email accounts or personal messaging services to communicate with pupils. Professional communication with parents/carers must take place through approved school channels such as ClassDojo, Arbor or school email.

Staff must not use personal mobile phones, personal tablets, personal cameras or other personal devices to photograph or record pupils. Photographs and recordings for school purposes must be made using school-owned or specifically authorised equipment and handled in accordance with parental consent/preferences, the Data Protection Policy and safeguarding requirements.

[Staff personal devices, images and recordings](#)

Staff using work devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others.

They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must report this promptly to the Headteacher and/or JC Comtech and follow the school's data-breach procedures where relevant.

Work devices must be used solely for work activities.

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 the behaviour 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

The school will maintain appropriate cyber-security measures in conjunction with JC Comtech, including secure individual accounts, access controls, software and security updates, backups and incident-response arrangements. Staff must report suspected phishing, malware, compromised accounts, loss of devices or data, and other cyber-security concerns promptly. Safeguarding and data-protection implications will be considered together where an incident affects pupils or personal data. Security controls will be reviewed as systems and DfE cyber-security standards develop.

Cyber security and data protection

Training

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).

The DSL 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 records online safeguarding concerns and actions on MyConcern in line with the school's Safeguarding and Child Protection Policy. Mrs Lucy Smith reviews the daily JC Comtech filtering and monitoring report and records safeguarding concerns, actions and outcomes on MyConcern where appropriate. Online-safety themes and incidents are

reviewed to identify patterns, training needs and necessary changes to controls, curriculum provision or technical settings.

This policy will be reviewed at least annually and sooner if there are significant changes to statutory guidance, technology, the school's systems or safeguarding risks. Filtering and monitoring provision will also be formally reviewed at least annually and after significant incidents or material system changes. The governing body will approve the policy and receive assurance about implementation.

Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Anti-Bullying Policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Acceptable Use policy
- Staff Code of Conduct
- Mobile Phone / Personal Device arrangements
- Computing, PSHE and RSE curriculum documentation

Appendix 1: 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 using the school's iPads, laptops, school accounts, email and internet, I will use technology safely, respectfully and responsibly. I will: • use my own school username and password and keep my password private • use school email and online services only for learning and other purposes approved by staff • not try to bypass filtering, monitoring or security controls • not access, create or share harmful, bullying, discriminatory, sexual or otherwise inappropriate content • not share personal information about myself or others without permission • tell a trusted adult straight away if something online worries, upsets or harms me or someone else • not use generative AI tools in school unless the school has specifically authorised a supervised activity. Mobile phones and personal devices: • I will only bring a mobile phone to school if I am in Year 5 or 6, it is needed for travel to/from school and written parental/carers permission has been given. • I will switch it off and hand it to the school office on arrival so it can be signed in and stored securely. • I will not use or access it during the school day or school-organised clubs/activities unless the Headteacher has authorised an exception. • I will not bring or wear a smartwatch at school. I understand that JC Comtech provides the school's filtering and monitoring and that activity on school systems may be monitored to help keep everyone safe. I will always use school technology responsibly.	
Signed (pupil):	Date:
Parent/carers 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 for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carers):	Date:

Appendix 2: acceptable use agreement (staff, governors, volunteers and visitors)

Acceptable use of the school's ICT systems and the internet: agreement for staff, governors, volunteers and visitors	
Name of staff member/governor/volunteer/visitor:	
When using the school's ICT systems, internet, school devices or approved online services, I will: • use them professionally, lawfully and in accordance with safeguarding, data-protection and cyber-security requirements • use official school systems for professional communication with pupils and parents/carers, including ClassDojo, Arbor and school email as appropriate • not use personal devices to photograph or record pupils and not use personal social-media, email or messaging accounts to communicate with pupils • use only authorised accounts, software, cloud services and AI tools; Microsoft Copilot within the school's Microsoft 365 environment may be used by staff for planning and resource creation • check AI-generated material for accuracy, bias, copyright, safeguarding and age-appropriateness and remain professionally responsible for the final content • not place safeguarding information, special-category data or confidential/personal information into AI services unless that specific processing has been approved by the school • keep passwords secure, use only my own account and not attempt to bypass filtering, monitoring or security controls • report safeguarding concerns immediately to the DSL/ADSL and report filtering, cyber-security or data-protection incidents through the school's agreed procedures.	
I understand that the school uses proportionate filtering and monitoring arrangements to safeguard users and systems. I will take reasonable steps to keep school devices and data secure, follow the school's Data Protection Policy and Staff Code of Conduct, and remain professionally responsible for checking the accuracy and suitability of any AI-generated material I use. I will model safe, responsible and professional online behaviour and ensure pupils in my care do the same.	
Signed (staff member/governor/volunteer/visitor):	Date: