



Online Safety Policy

Date Reviewed/Updated: August 2026

Next Review: September 2027

Every Child, Every Chance, Every Day; Working Together

Writing, monitoring and reviewing the e-safety policy

Development of the policy

This online safety policy relates to other policies including those for computing, safeguarding, anti-bullying, curriculum policies and data protection and security. This online safety policy has been written on behalf of the school by the computing subject leader, who is also the designated online safety co-ordinator; in consultation with the headteacher, safeguarding team, staff (including teachers, support staff and technical staff), governors, parents/carers and pupils.

Reviewing the policy

- The policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of new technologies, new threats to online safety or incidents that have taken place.
- The next review date is September 2027.

Monitoring the impact of the policy

- A log will be maintained to record reported incidents.
- Serious incidents will be referred to the appropriate authorities.

Scope of the Policy

This policy applies to all members of the school community (including staff, governors, pupils, volunteers, parents/carer, visitors, and community users) who have access to and are users of school IT systems, both in and out of the school.

Roles and Responsibilities

Governors

Governors are responsible for reviewing the effectiveness of the online safety policy.

Headteacher and Senior Leaders

The headteacher has a duty of care for ensuring the safety (including online safety) of the members of the school community.

- The day to day responsibility for online safety will be delegated to the online safety co-ordinator
- The headteacher and members of the senior leadership team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.

Online Safety Co-ordinator

- Takes day to day responsibility for online safety issues in liaison with the designated safeguarding lead co-ordinator and has a leading role in establishing and reviewing the school online safety policy.
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- Provides training and advice for staff.

- Liaises with the IT technician.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments (in conjunction with the safeguarding team).
- Reports regularly to the headteacher.
- Sources leaflets and letters that can be accessed by all staff to support parents/carers with any issues that may arise.
- Communicate online safety tips with parents/carers through letters and the school's communication app.
- **Provides half termly assemblies to the whole school about all elements of cybersafety/e-safety/online safety.**

The IT Provider (Wolvern IT and Schools IT)

Are responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Local Authority e-safety guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering service applied is appropriate, effective and reasonable and is updated on a regular basis.
- that 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.
- that the use of the network / internet / remote access / email is monitored in order that any misuse or attempted misuse can be identified.

Teaching and Support Staff

Are responsible for ensuring that:

- they have an up to date awareness of online safety matters and of the current school online safety policy and practices.
- they have read, understood and signed the Acceptable Use Agreement.
- they report any online safety issues via the online safety log or in the case of serious incidents to the headteacher for investigation. These may also need reporting to the safeguarding lead, depending on the nature of the issue.
- they report any GDPR breaches to the DPO.
- all digital communications with pupils and parents/carers should be 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.
- all children can identify a trusted adult who they can inform of any issues online.
- dedicated e-safety/online safety lessons are taught to children in line with the curriculum e-safety objectives.
- pupils understand and follow the online safety and acceptable use policies.
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities and implement current policies with regard to these devices.
- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that any unsuitable material that is found in internet searches is logged so that filtering can be updated.

Designated Safeguarding Lead Co-ordinator

Is trained in online safety issues and aware of the potential for serious child protection / safeguarding issues that can arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate online contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying
- exposure to propaganda

Pupils

- Are responsible for using the school digital technology systems in accordance with the school acceptable use rules and online safety guidance.
- Should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- Will be expected to know and understand school rules around online safety. These are outlined in their behaviour contracts and on classroom posters.
- Are responsible for keeping their passwords for online platforms safe in their reading diaries. They should tell their teacher if they lose their diary so that their passwords can be changed.
- 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.

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. During the admissions process, parents/carers are presented with the children's acceptable use policy and should read through these with their children, signing to acknowledge their understanding and responsibility for this. The school will take every opportunity to help parents/carers understand these issues through training events, newsletters, admissions paperwork, letters, website and the school's communication app.

Parents/carers are encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events.

Parents/carers are encouraged to speak to the school if they have any concerns with their children or their children's friends online.

Education, training and communicating of online safety messages

Pupils

Why the Internet and digital communications are important

- The internet is an essential element in 21st century life for education, business and social interaction. The school recognises it has a duty to provide pupils with high-quality internet access as part of their learning experience in school and prepare them to make safe and effective use out of school.
- Internet use is part of the statutory curriculum and a necessary tool for staff and pupils.

Online safety (e-safety)

The school recognises that whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

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 will be provided as part of computing / PSHE / other lessons and will be regularly revisited.
- Key online safety messages should be reinforced as part of a planned programme of assemblies and other class and whole school activities.
- E-safety (online safety) rules will be displayed in all classrooms and the children will sign to say they understand these as part of their behaviour contract at the start of each academic year.
- Details of how to respond to concerns will be posted in all rooms where computers are used.
- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils should be encouraged to adopt safe and responsible use both within and outside school.
- Pupils will be taught how to keep themselves safe online both in and out of school and how to respond to concerns regarding unpleasant content or inappropriate contact.
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices.
- 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 monitoring the content of the websites the young people visit.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, and discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the IT Technician can temporarily remove those sites from the filtered list for the period of study.

Parents/carers and the wider community

The school recognises the essential role parents/carers play in the monitoring and regulation of children's online behaviours out of school and that they may underestimate the dangers. The school will therefore seek to provide information and awareness to parents/carers through information evenings, letters/ newsletters/ web site, curriculum activities, providing literature and drawing their attention to high profile events and campaigns. These events and resources will also be made available as appropriate to the wider community.

Staff and volunteers

- An audit of the online safety training needs of all staff will be carried out yearly. Staff training will be carried out where necessary to ensure all staff are aware of current issues. This may be overlapped with yearly safeguarding training.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school's online safety policy and Acceptable Use Agreements.
- The online safety co-ordinator will provide advice, guidance or training to individuals as required.

Governors

Governors should take part in online safety training or awareness sessions (in particular those governors responsible for technology, online safety or safeguarding).

Technical – infrastructure / equipment, filtering and monitoring

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- Pupils will have a class log on.
- The administrator passwords for the school ICT system is kept by the IT Provider.
- The school is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users.

- An appropriate system is in place for users to report any actual / potential technical incident / security breach.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software.
- 'Guests' (for example, visitors and supply teachers) are not allowed access to secure parts of the network and can only access using class log ins. Trainee teachers undergoing a placement of 6 weeks or more are given a log in to access the network, but not be given access to Arbor. This access is removed once the placement is finished.
- Only the IT Provider is able to install programmes on school devices.

At Crabtree Farm Primary we ensure that we meet the Digital and Technology Standards as detailed in the DFE publication 'Meeting digital and technology standards in school'. Meeting digital and technology standards in schools and colleges – Filtering and monitoring standards for schools and colleges – Guidance – GOV.UK (www.gov.uk). We complete an annual audit of the filtering and monitoring provision in school, in line with the guidance.

The filtering set up at Crabtree Farm is as follows:

- The internet filtering services are provided and supported by Ekte.
- The main internet filtering used on desktops, staff laptops and iPads is provided by Ekte using the iBoss platform. The filtering is split into two levels (staff and students).
- All shared iPads have student level filtering applied to them.
- There is a pool of DfE supplied laptops provided for revision purposes to Year 6/identified pupils, which have internet filtering in place provided by Ekte using the iBoss platform. The iBoss product is installed to provide filtering on these laptops whilst being used at home or on infiltrating internet connections outside of the school network.

The monitoring set up at Crabtree Farm is as follows:

- Weekly safeguarding reports for students and staff are generated by Ekte through the iBoss platform and are emailed to the safeguarding team.
- Ekte generates real time alert emails to the safeguarding team from the iBoss product, in relation to any high risk keywords.
- The safeguarding team checks the reports/alerts and address any concerns, following the safeguarding policy.
- Staff delivering any lessons/activities involving online platforms carry out ongoing monitoring when children are using devices.
- Monitoring 'tester' checks of the filtering system are carried out periodically by the IT support and safeguarding team; and logged. Any issues are addressed as appropriate.
- Staff are responsible for knowing which ipad/computer each child has logged on to and when (as shared log ins are used per year group) in order to determine who was using devices, so that any filtering and monitoring

concerns can be responded to with the appropriate child. Staff log on via individual log ons.

Managing Emerging Technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- All staff should note that technologies such as mobile phones with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Publishing Content

Use of Digital and Video Images and Pupils' work

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents/carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Parents/carers are welcome to take videos and digital images of their children only at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on social networking sites, nor should parents/carers comment on any activities involving other pupils in the digital/video images.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Photographs published on the website, or elsewhere that include pupils will be selected carefully, preferably using group photographs rather than photographs of individual children, and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Published Content and the School Website

The contact details on the school website should be the school address, email and telephone number. Staff or pupil's personal information must not be published. The head teachers will take overall editorial responsibility and ensure that content is accurate and appropriate.

Communications

Email

- Email should be sent using the approved Schools IT service, which is regarded as safe and secure and is monitored.
- Users must immediately report, 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.
- Any digital communication between staff and pupils or parents/carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- If required as part of a learning activity, whole class email addresses may be used.
- Pupils should be taught about the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Blogging

- Pupils will be explicitly taught about responsible and courteous behaviour while blogging and commenting on blogs and will sign an agreement before being allowed to use an approved blog.
- They will be warned that once they have posted a blog or comment they will not be able to remove it, and there will be consequences for inappropriate blogging or commenting.
- Staff will monitor blogs and comments posted and deal with any incidents of inappropriate posting.

Social Networking

Protection of Pupils

Whilst pupils will not be allowed access to social networking sites in school, it is very possible that they will have access from home. As part of their online safety curriculum, they will be taught about the potential dangers posed by such sites and opportunities to communicate with strangers. This will include:

- never to give out personal details of any kind which may identify them, their friends or their location.
- not to place personal photos on any social network space without considering how the photo could be used now or in the future.
- to only invite known friends and deny access to others when using social networking and instant messaging services. Pupils will be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications.
- Pupils will be taught about how to respond to any inappropriate contact.

Use by Staff

- As part of their online safety training staff will receive guidance on acceptable use, social media risks, checking of privacy settings, data protection and reporting issues.
- School staff should ensure that no reference is made in social media to pupils, parents/carers or school staff.
- Staff should ensure that they do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions expressed by staff on social media should not be attributed to the school or local authority.
- Security settings on personal social media profiles should be regularly checked to minimise the risk of loss of personal information.

Data Protection

Personal data will be recorded, processed, transferred and made available according to UK General Data Protection Regulations (see UK GDPR Policy for more information).

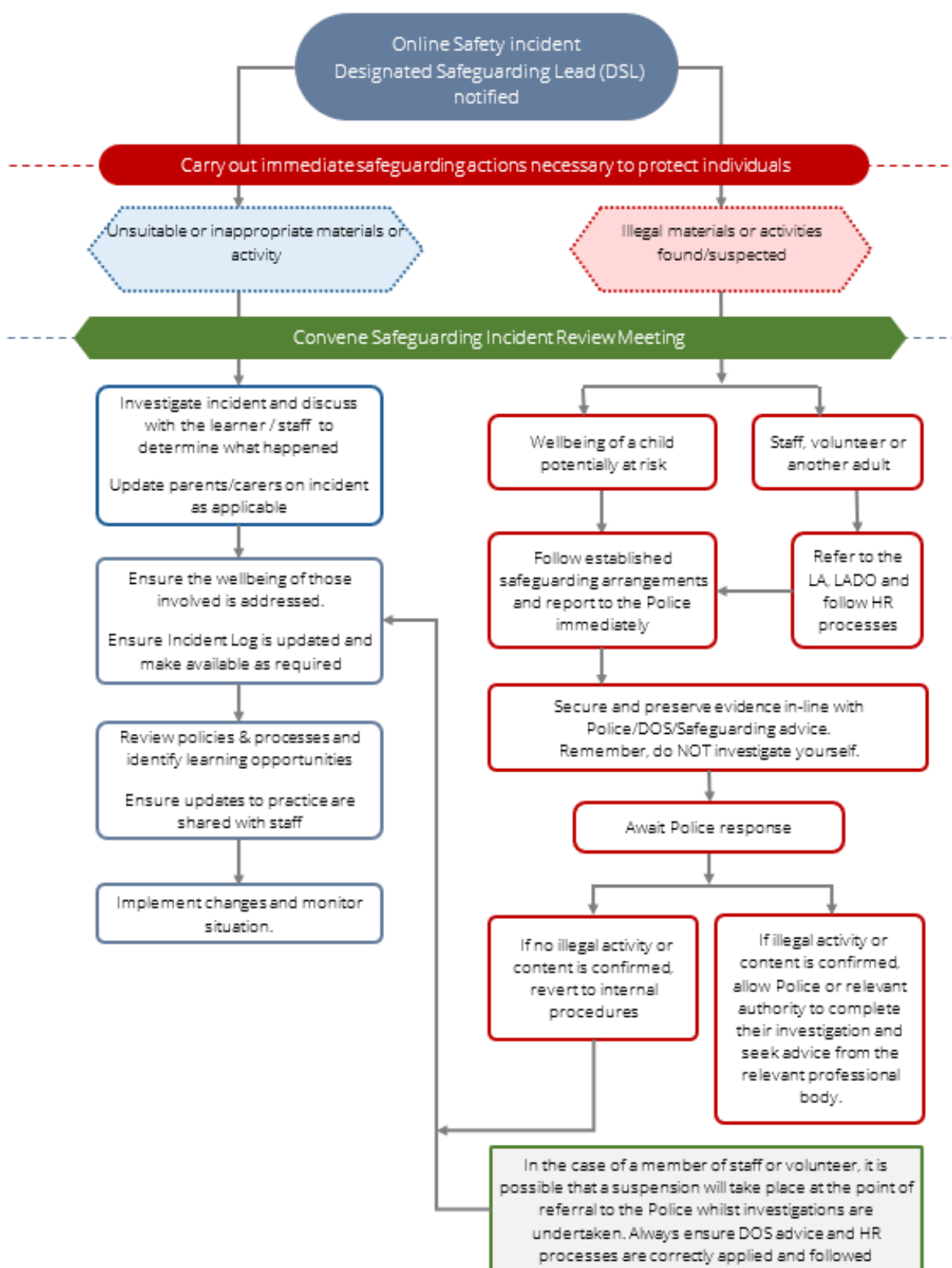
Staff must ensure that they:

- Take care at all times to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data (e.g. on memory sticks) using encryption and secure password protected devices.
- Ensure school laptops are password protected.

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right-hand side of the flowchart for responding to online safety incidents and report immediately to the police.



Other Incidents

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority or national / local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of child abuse then the monitoring should be halted and referred to the police immediately. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - other criminal conduct, activity or materials

It is important that all of the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions

- Most incidents are likely to involve inappropriate rather than illegal misuse. It is important that any incidents are logged and dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.
- It is intended that incidents of misuse involving pupils will be dealt with through normal behaviour / disciplinary procedures.

Use of Artificial Intelligence (AI)

Generative AI (Gen AI) is developing rapidly and its use in education is increasing. In schools, AI is typically used in three areas: learner support, teacher support, and school operations. All use must be safe, ethical and responsible.

We recognise that Gen AI can introduce risks. These risks can be reduced through our existing safeguarding, data protection and technical security arrangements, and by updating procedures where needed. Safeguarding of pupils and staff remains central to our approach.

The school will:

- Support appropriate use of AI to enhance learning and teaching, improve outcomes, streamline administration and reduce workload. Staff remain professionally responsible and accountable for any work supported by AI.
- Comply with relevant law and guidance, including Keeping Children Safe in Education (KCSIE) and UK GDPR.
- Provide training and guidance for staff and governors on the benefits, risks and safe use of AI, and identify further development needs.
- Teach about AI through the curriculum where appropriate, helping learners understand how Gen AI works, its benefits and limitations, and its ethical and social impacts.

Safe use, data protection and security

The school will:

- Protect personal and sensitive data. Staff must not enter personally identifiable or sensitive information into AI tools. Where AI is used, staff should use anonymised data only.
- Require UK GDPR compliance. Staff must ensure any AI tool used meets data protection and security requirements before use.
- Approve tools and accounts. Only school-approved AI tools may be used for schoolwork, and staff should use school-provided AI accounts where available to support oversight and reduce risk.
- Safeguard sensitive information. Internal documents, strategic plans or other sensitive material must not be entered into third-party AI tools unless the tool and purpose have been explicitly approved.

Quality, fairness and integrity

The school will:

- Maintain human oversight. AI may support work but must not replace professional judgement—especially in decisions that affect people. AI outputs must be checked for accuracy before sharing or publishing.
- Promote transparency. Where AI has materially supported an output (e.g. documents, presentations, communications), staff should make this clear where appropriate.
- Address bias and discrimination. We recognise AI outputs may reflect bias. The school will use appropriate safeguards, review processes and procurement checks to prioritise fairness and safety.
- Protect copyright and intellectual property. The school will take steps to avoid copyright infringement and protect the intellectual property of staff and pupils, including ensuring pupils' work is not used to train AI systems without appropriate consent.

Reporting, monitoring and accountability

The school will:

- Require prompt reporting of AI-related concerns, including misuse, data incidents or inappropriate outputs, to the headteacher and DPO.
- Maintain an inventory of AI tools in use, with purposes and risks recorded, and carry out regular review.
- Engage parents/carers with clear information about how AI is used in school.

Use in assessment and feedback

AI tools may be used to support teachers with assessment processes (e.g. identifying areas for improvement and drafting feedback), and to support pupils in improving their work. Teachers remain responsible for outcomes and must ensure accuracy, fairness and appropriate use.

Misuse and disciplinary action

Improper use of AI; including breaches of this policy, data protection failures, misuse of sensitive information, or failure to follow agreed processes, may result in action under the school's Staff Disciplinary Policy.

This policy will be reviewed by the computing subject leader and leadership team; and shared with all stakeholders.

Mrs Carlton

Computing Subject Leader and Online Safety Co-ordinator

August 2026, to be reviewed in September 2027

We have in place a group of policies that complement each other to safeguard, protect and promote the welfare of our children. These policies are:

- Behaviour Policy
- Complaints Procedure
- SEND Policy
- Safeguarding Policy
- UK GDPR Policies, including Acceptable Use Policy and Remote Access Mobile Computing Policy
- Visitor and Volunteer Policy
- Whistle Blowing Procedure
- Whole School Code of Conduct

Appendix 1

The school E-Safety Rules poster. This is shared with children regularly and displayed near all computing equipment in school.

