



Introduction

Online safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. This policy sets out the approach of Isbourne Valley School to the need to:

- educate children and young people about the benefits and risks of using new technology;
- provide robust processes and safeguards to secure the online safety of pupils, staff, volunteers and governors;
- identify and support groups of pupils that are potentially at greater risk of harm online than others;
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones'); and
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

We understand the valuable potential that artificial intelligence (AI), including generative AI, holds for schools. It can, for example, be used to enhance teaching methods, customise learning experiences and progress educational innovation. We are also aware of the risks posed by AI, including data protection breaches, copyright issues, ethical complications, safeguarding and compliance with wider legal obligations. AI tools include generative chatbots such as ChatGPT, CoPilot and Google Gemini (please note, these are examples and other tools exist and will be created – these are also covered by this policy). This policy sets out the approach of Isbourne Valley School to:

- supporting the use of AI to enhance teaching and learning;
- supporting staff to explore AI solutions to improve efficiency and reduce workload;
- preparing staff, governors and pupils for a future in which AI technology will be an integral part;
- promoting equity in education by using AI to address learning gaps and provide personalised support;
- making sure that AI technologies are used ethically and responsibly by all staff, governors and pupils; and
- protecting the privacy and personal data of staff, governors and pupils in compliance with the UK GDPR

This policy applies to all members of the Isbourne Valley School community (including staff, pupils, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in and out school.

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

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

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, [Keeping Children Safe in Education](#), and its advice for schools, together with that published by Ofsted and the Joint Council for Qualifications, on:

- [Teaching online safety in schools](#)
- [Meeting digital and technology standards](#)
- [Preventing and tackling bullying](#) and
- [Relationships and sex education](#)

- [Searching, screening and confiscation](#)
- [Mobile phones in schools](#)
- [Generative artificial intelligence \(AI\) in education](#)
- [Generative AI: product safety standards](#)
- [How Ofsted looks at AI during inspection and regulation](#)
- [AI use in assessments](#)

It also refers to the DfE's guidance on [protecting children from radicalisation](#).

It reflects existing legislation, including but not limited to the [Education Act 1996](#) (as amended), the [Education and Inspections Act 2006](#), the [Children's Wellbeing and Schools Act 2026](#), the [Equality Act 2010](#), [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#), the [Data Protection Act 2018 \(DPA 2018\)](#) and the [Data \(Use and Access\) Act 2025](#). In addition, it reflects the [Education Act 2011](#), which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

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

Governors

Governors are responsible for the approval and monitoring of the Online Safety Policy, holding the Headteacher to account for its implementation and for reviewing the effectiveness of the policy. The governing body will make sure that online safety is a running and interrelated theme in the whole-school approach to safeguarding and related policies and procedures, including when planning the curriculum, teacher training, the role of the DSL (and deputies) and any parental engagement. The governing body will:

- make sure all staff undergo online safety training as part of child protection and safeguarding training;
- make sure all staff understand the expectations, roles and responsibilities around filtering and monitoring;
- make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, so that they are continually provided with the relevant skills and knowledge to effectively safeguard children;
- hold the Headteacher to account for the implementation of this policy in line with the school's AI strategy;
- make sure the Headteacher and Online Safety Lead are appropriately supported to make informed decisions regarding the effective and ethical use of AI in the school;
- follow the guidelines below to protect data when using generative AI tools:
 - use only approved AI tools (see below and appendix);
 - seek advice from the data protection officer, Online Safety Lead and the designated safeguarding lead, as appropriate;
 - check whether they are using an open or closed generative AI tool;
 - make sure there is no identifiable information included in what they put into [open](#) generative AI tools (unless strictly necessary and they have been approved to do so – check with your DPO/AI lead where appropriate);
 - acknowledge or reference the use of generative AI in their work; and
 - fact-check results to make sure the information is accurate
- co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL);
- make sure children are taught how to keep themselves and others safe, including keeping safe online;
- make sure the school has appropriate filtering and monitoring systems in place on school devices and school networks and that a review of the effectiveness of the filtering and monitoring systems is carried out by the Headteacher (with the IT support team as appropriate) at least once every academic year. The governing body will review the [DfE filtering and monitoring standards](#), and discuss with IT staff and service providers what needs to be done to support the school in meeting the standards, which include:
 - identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
 - reviewing filtering and monitoring provisions at least annually;
 - blocking harmful and inappropriate content without unreasonably impacting teaching and learning; and
 - having effective monitoring strategies in place that meet their safeguarding needs.

All governors will:

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

The governing body may delegate some of these functions to the Teaching & Learning Committee and/or the individual governor nominated as 'Online Safety Governor'. The nominated Online Safety Governor is Rachel Bale.

Headteacher

The Headteacher is responsible for making sure that staff understand this policy, and that it is being implemented consistently throughout the school. The Headteacher will make sure that there are robust cover arrangements for when the DSL is unavailable due to illness, leave or other circumstances to make sure safeguarding concerns are received, monitored and acted on without delay.

The Headteacher is also responsible for the day-to-day leadership and management of AI use in the school and will:

- liaise with the data protection officer (DPO) to ensure that the use of AI is in accordance with data protection legislation;
- liaise with the DSL to ensure that the use of AI is in accordance with Keeping Children Safe in Education and the school's safeguarding policy;
- make sure that the guidance set out in this policy is followed by all staff;
- review and update this policy as appropriate, and at least annually;
- make sure staff are appropriately trained in the effective use and potential risks of AI;
- make sure pupils are taught about the effective use and potential risks of AI; and
- sign off on approved uses of AI, or new AI tools, taking into account advice from the DPO, the Network Manager, the Online Safety Leader, and data protection impact assessments.

Online Safety Leader

Isbourne Valley School will have a named member of staff with day-to-day responsibility for online safety including the day-to-day leadership, ownership and management of AI use in the school, who:

- has a leading role in establishing and reviewing the school Online Safety policies/documents;
- makes sure 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 Local Authority/relevant body;
- liaises with school Network Manager;
- receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments;
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs;
- attends relevant meeting/committee of governors;
- reports regularly to headteacher and governors.

Investigation into incidents will be dealt with by the Online Safety Leader, with sanctions being the responsibility of the Headteacher.

Network Manager/Technical Support

Isbourne Valley has a managed ICT service provided by Winchcombe School. It is the responsibility of the Online Safety Leader to ensure that the Network Manager carries out all the Online Safety measures that would otherwise be the

responsibility of the school technical staff, as suggested below. It is also important that the Network Manager is fully aware of the Online Safety policy and procedures.

The Network Manager, Technical Staff, Schools Broadband (Isbourne Valley School's broadband provider) and Computing Leader are responsible for making sure that:

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

This list is not intended to be exhaustive.

Staff and Volunteers

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

- having an understanding of this policy;
- consistently implementing this policy;
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 3), and making sure that pupils follow the school's terms on acceptable use (appendices 1 and 2);
- knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing to the DSL and using the My Concern system;
- following the correct procedures by informing the headteacher and ICT manager if they need to bypass the filtering and monitoring systems for educational purposes;
- working with the DSL to ensure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy;
- making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;
- responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

- As part of our aim to reduce staff workload while improving outcomes for our pupils, we encourage staff to explore opportunities to meet these objectives through the use of approved AI tools. Any use of AI must follow the guidelines set out in this policy. To protect data when using generative AI tools, staff must:
- use only approved AI tools (see below and appendix)
- seek advice from the DPO /Network Manager/Headteacher/Online Safety Lead, as appropriate
- report safeguarding concerns to the DSL in line with our Safeguarding Policy
- check whether they are using an open or closed generative AI tool
- make sure there is no identifiable information included in what they put into open generative AI tools
- acknowledge or reference the use of generative AI in their work
- fact-check results to make sure the information is accurate

All staff play a role in making sure that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

Designated Safeguarding Lead and Deputy

The Designated Safeguarding Lead (DSL), and Deputy, should be trained in Online Safety issues and the use of AI and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data;
- access to illegal/inappropriate materials;
- inappropriate on-line contact with adults/strangers;
- potential or actual incidents of grooming;
- cyber-bullying;
- the use of existing and emerging AI tools.

It is important to emphasise that these are child protection issues, not technical issues, and simply that the technology provides additional means for child protection issues to develop.

The responsibilities of the DSL (and Deputy) are set out in our Safeguarding Policy.

The DSL takes lead responsibility for online safety in school, including in particular but not limited to:

- supporting the Headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- working with the Headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- understanding the filtering and monitoring systems and processes in place on school devices and school networks
- working with the ICT manager to make sure the appropriate systems and processes are in place
- working with the Headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- managing all online safety issues and incidents in line with the school's safeguarding policy
- responding to safeguarding incidents in line with KCSIE and the school's safeguarding policy
- making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- updating and delivering staff training on online safety including AI safeguarding threats (appendix 4 contains a self-audit for staff on online safety training needs)
- liaising with other agencies and/or external services if necessary
- providing regular reports on online safety in school to the headteacher and/or governing body
- carrying out annual risk assessments that consider and reflect the risks children face
- being aware of new and emerging safeguarding threats posed by AI
- providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

The DSL (and deputy) 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.

Pupils

It is important that children have awareness and understanding of the importance of online safety and the use of AI. Pupils are therefore expected, in a way that is appropriate to their age and development, to:

- be responsible for using the school's digital technology systems in accordance with our Acceptable User Policy;
- understand the importance of reporting abuse, misuse or access to inappropriate materials, know how to do so, and to do so;
- know and follow the school's rules on the use of mobile devices and digital cameras;
- know and understand about taking and using digital images, and about cyber-bullying;
- understand the importance of following good Online Safety practice out of school;
- follow the guidelines in this policy; and
- understand that this policy covers their actions out of school if those are related to their being a member of the school community.

Parents/Carers

Parents and carers play a crucial role in making sure that their children understand the need to use the internet and mobile devices in an appropriate way. We work together with parents and carers to promote good Online Safety practice. Parents and carers are expected to:

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

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

- What are the issues? – [UK Safer Internet Centre - https://saferinternet.org.uk/](https://saferinternet.org.uk/)
- Hot topics – [Childnet](#)
- Parent resource sheet – [Childnet](#)
- [Childline](#) –
- <https://www.childline.org.uk/info-advice/bullying-abuse/online-safety/online-mobility/online-safety/staying-safe-online/>
- [Internet matters - https://www.internetmatters.org/](https://www.internetmatters.org/)

Visitors and members of the community

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

Data protection officer (DPO)

The data protection officer (DPO) is responsible for monitoring and advising on our compliance with data protection law, including in relation to the use of AI.

Our DPO is Rachel Bale and is contactable via the school office or by email: chair@isbournevalleyschool.com.

Education

Pupils

The education of pupils in Online Safety, including about how they can take a responsible approach themselves, is an essential and important part of our Online Safety provision. We know that children need information, help and support to understand, recognise and avoid Online Safety risks. Online Safety messages are therefore repeated and reinforced regularly as part of everyday school life and the Online Safety curriculum and the wider curriculum generally.

Pupils will be taught about online safety as part of the curriculum. Teaching about safeguarding, including online safety, will be adapted, where necessary, for vulnerable children, victims of abuse and some pupils with SEND. All primary schools have to teach [Relationships education and health education](#).

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

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 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
- Be discerning in evaluating digital content

By the **end of primary school**, pupils will know:

- That people should be respectful in online interactions, and that the same principles apply to online relationships as to face-to-face relationships, including where people are anonymous. For example, the importance of avoiding putting pressure on others to share information and images online, and strategies for resisting peer pressure
- How to critically evaluate their online relationships and sources of information, including awareness of the risks associated with people they have never met. For example, that people sometimes behave differently online, including pretending to be someone else, or pretending to be a child, and that this can lead to dangerous situations. How to recognise harmful content or harmful contact, and how to report this
- That there is a minimum age for joining social media sites, which protects children from inappropriate content or unsafe contact with older social media users, who may be strangers, including other children and adults
- The importance of exercising caution about sharing any information about themselves online. Understanding the importance of privacy and location settings to protect information online
- Online risks, including that any material provided online might be circulated, and that once a picture or words has been circulated there is no way of deleting it everywhere and no control over where it ends up
- That the internet contains a lot of content that can be inappropriate and upsetting for children, and where to go for advice and support when they feel worried or concerned about something they have seen or engaged with online

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The physical security of devices
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyber-bullying and the risks of online radicalisation.

Parents and Carers

Technology is a fast-changing part of all of our lives. Our pupils encounter devices, formats and platforms which did not exist when we were children. We will take every opportunity to provide information, raise awareness and help parents and carers understand these issues through parents' evenings, parents' information and workshop sessions, using and publicising high profile events such as Safer Internet Day newsletters, letters, highlighting relevant websites and publications, the school website and information about local and national Online Safety campaigns and literature. Parents and carers are encouraged to talk to the school if they have any questions about this policy or online safety and to raise any concerns with the headteacher and/or DSL.

Staff

It is important and essential that all staff receive Online Safety training and understand their responsibilities as outlined in this policy. Training will cover safe internet use, online safeguarding issues, including cyber-bullying, and the risks of online radicalisation. All staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
 - Abusive, threatening, harassing and misogynistic messages
 - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
 - sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse;

- develop the ability to make sure pupils can recognise dangers and risks in online activity and can weigh up the risks;
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

Training will be offered:

- as a planned programme of formal Online Safety training which is regularly updated and reinforced. An audit of the Online Safety training needs of all staff will be carried out regularly. It is expected that some staff will identify Online Safety as a training need within the performance management process;
- to all staff members as a refresher 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);
- to all new staff part of their induction programme;
- through external training events and by reviewing guidance documents released by relevant organisations;
- in staff meetings and INSET days;
- on an individual basis as required.

Governors

Governors will take part in Online Safety training and awareness sessions. This may be in a number of ways such as:

- Attendance at training provided by the Local Authority, National Governors Association or other relevant organisation;
- Participation in school training/information sessions for staff or parents, including assemblies and lessons.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of a person or group by another person or group, where the relationship involves an imbalance of power. To help prevent cyber-bullying, we will make sure that:

- pupils understand what it is and what to do if they become aware of it happening to them or others;
- pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim;
- we actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be;
- find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate;
- all staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training;
- we send information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained. The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- poses a risk to staff or pupils, and/or
- is identified in the school rules as a banned item for which a search can be carried out, and/or
- is evidence in relation to an offence.

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- make an assessment of how urgent the search is, and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher/DSL;
- explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it;
- seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so. When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- cause harm, and/or
- undermine the safe environment of the school or disrupt teaching, and/or
- commit an offence.

If inappropriate material is found on the device, it is up to Headteacher, in discussion with the DSL, to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- they reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- the pupil and/or the parent/carers refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), including any image generated or altered by AI, they will not:

- view, copy, print, share, store, save, forward on, or ask a child to share or download, the image;
- delete the image or ask the pupil to delete the image
- ask the pupil(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL
- share information about the incident with other members of staff, the pupil(s) it involves or their, or other, parents and/or carers
- say or do anything to blame or shame any pupil involved

The staff member will confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on [screening, searching and confiscation](#) and the UK Council for Internet Safety (UKCIS) guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#).

If the staff member has already viewed the imagery by accident (e.g. if the pupil showed it to them before they could ask them not to), they will report the incident to the DSL and seek support.

Any searching of pupils will be carried out in line with the DfE's latest guidance on [searching, screening and confiscation](#), UKCIS guidance on [sharing nudes and semi-nudes: advice for education settings working with children and young people](#) and our behaviour policy.

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

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils, parents and carers may be familiar with generative chatbots such as ChatGPT, CoPilot and Google Gemini. They can be 'open' or 'closed', which means:

- **Open generative AI tools** are accessible and modifiable by anyone. They may store, share or learn from the information entered into them, including personal or sensitive information
- **Closed generative AI tools** are generally more secure, as external parties cannot access the data you input

We follow the 5 principles set out in the [AI regulation white paper](#).

REGULATORY PRINCIPLE	WE WILL ...
Safety, security and robustness	• Make sure that AI solutions are secure and safe for users and protect users' data • Make sure we can identify and rectify bias or error • Anticipate threats such as hacking
Appropriate transparency and explainability	• Be transparent about our use of AI, and make sure we understand the suggestions it makes
Fairness	• Only use AI solutions that are ethically appropriate, equitable and free from prejudice – in particular, we will fully consider any bias relating to small groups and protected characteristics before using AI, monitor bias closely and correct problems where appropriate
Accountability and governance	• Make sure that the governing board and staff have clear roles and responsibilities in relation to the monitoring, evaluation, maintenance and use of AI
Contestability and redress	• Make sure that staff are empowered to correct and overrule AI suggestions – decisions should be made by the user of AI, not the technology • Allow and respond appropriately to concerns and complaints where AI may have caused error resulting in adverse consequences or unfair treatment

We recognise that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

We are aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:

- Sexual grooming
- Sexual harassment
- Sexual extortion
- Child sexual abuse/exploitation material
- Harmful content
- Harmful advertisements and promotions
- Bullying

Where there are safeguarding concerns arising from the use of generative AI, a report must be made to the DSL immediately. Any such incident will be dealt with according to the procedures set out in our safeguarding policy and in accordance with our child protection and safeguarding processes.

We will treat any use of AI to bully pupils in line with our Anti-bullying and Behaviour policies.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Staff and governors' use of AI

Approved use of AI

We are committed to helping staff and governors reduce their workload while improving outcomes for our pupils. Generative AI tools can make certain written tasks quicker and easier to complete, but cannot replace the judgement and knowledge of a human expert. Whatever tools or resources are used to produce plans, policies or documents, the quality and content of the final document remains the professional responsibility of the person who produced it. Any plans, policies or documents created using AI should be clearly attributed. Any member of staff or governor using an AI-generated plan, policy or document should only share the AI-generated content with other members of staff or governors for use if they are confident of the accuracy of the information, as the content remains the professional responsibility of the person who produced it.

Staff and governors must always consider whether AI is the right tool to use - just because the school has approved its use does not mean it will always be appropriate.

Any use of AI must follow the guidelines set out in this policy. To protect data when using generative AI tools, staff must:

- Use only approved AI tools (see below and appendix 6)
- Seek advice from the data protection officer/Online Safety lead/Network Manager/DSL, as appropriate
- Report safeguarding concerns to the DSL in line with our school's child protection and safeguarding policy
- Ensure there is no identifiable information included in what they put into generative AI tools (unless it is strictly necessary and they are approved to do so – they should check with the DPO/AI lead where appropriate)
- Acknowledge or reference the use of generative AI in their work
- Fact-check results to make sure the information is accurate

All staff play a role in ensuring that pupils understand the potential benefits and risks of using AI in their learning. All of our staff have a responsibility to guide pupils in critically evaluating AI-generated information and understanding its limitations.

Process for approval

Staff are welcome to suggest new ways of using AI to improve pupil outcomes and reduce workload. Staff should contact the Headteacher to discuss any ideas they may have with regards to using AI, so the Headteacher can take the suggestions forward if they deem it to be a satisfactory new method of working.

The Headteacher is responsible for signing off on approved uses of AI, or new AI tools.

Any use of generative AI by staff and pupils will be risk assessed, which will include plans for mitigating against unauthorised use cases. The intended use case will be specified and have clear benefits that outweigh the risks. As part of this process, we will seek assurances from suppliers of AI tools about how their products meet the DfE's [AI product safety standards](#).

If it is strictly necessary to use an AI tool to process personal data, we will carry out a data protection impact assessment (DPIA) in addition to the risk assessment. The DPO will advise on this. If the use case is approved, we will also update our privacy notices accordingly.

In the case of AI tools intended for use by pupils, the risk assessment process must consider:

- Age restrictions set by AI tools
- Statutory requirements of [KCSIE](#) and our child protection and safeguarding policy
- [Filtering and monitoring standards](#) to make sure we have the appropriate systems in place to protect pupils from harm

- The DfE's [AI product safety standards](#)

Data protection and privacy

To make sure that personal and sensitive data remains secure, no one will be permitted to enter such data into generative AI tools or chatbots that have not been approved as safe for this use case. If personal and/or sensitive data is entered into an unauthorised generative AI tool, Isbourne Valley School will treat this as a data breach and will follow the personal data breach procedure outlined in our data protection policy.

Intellectual property

Most generative AI tools use inputs submitted by users to train and refine their models. Pupils own the intellectual property (IP) rights to original content they create. This is likely to include anything that shows working out or is beyond multiple choice questions. In addition, materials created by teachers may be copyright material. Examples of what may be deemed original creative work include:

- Essays, homework or any other materials written or drawn by a pupil aside from multiple-choice questions responses
- Lesson plans created by a teacher
- Prompts entered into generative AI tools

We will not allow or cause intellectual property, including pupils' work, to be used to train generative AI models without appropriate consent or exemption to copyright. We are aware that secondary infringement could happen if AI products are trained on unlicensed material and outputs and then used in schools or published more widely, such as on the school's website. This may include:

- Publishing a policy that has been created by an AI tool that used input taken from another school's policy without that school's permission
- Using an image on a website that has been created by an AI tool using input taken from the copyright holder without their permission

Exemptions to copyright are limited – we will seek legal advice if we are unsure as to whether we are acting within the law.

Bias

We are aware that AI tools can perpetuate existing biases, particularly towards protected characteristics including sex, race and disability. For this reason, critical thought must be applied to all outputs of authorised AI applications. This means fact and sense-checking the output. We will make sure we can identify and rectify bias or error by training staff in this area. We also regularly review our use of AI to identify and correct any biases that may arise.

If parents/carers or pupils have any concerns or complaints about potential unfair treatment or other negative outcomes as a consequence of AI use, these will be dealt with through our usual complaints procedure.

Raising concerns

We encourage staff and governors to speak to the Headteacher in the first instance if they have any concerns about a proposed use of AI, or the use of AI that may have resulted in errors that lead to adverse consequences or unfair treatment.

Safeguarding concerns arising from the use of generative AI must be reported immediately to the DSL in accordance with our school's safeguarding policy.

Ethical and responsible use

We will always:

- use generative AI tools ethically and responsibly
- remember the principles set out in our school's equality policy when using generative AI tools
- consider whether the tool has real-time internet access, or access to information up to a certain point in time, as this may impact the accuracy of the output
- fact and sense-check the output before relying on it

Staff and governors must not:

- generate content to impersonate, bully or harass another person
- generate explicit or offensive content
- input offensive, discriminatory or inappropriate content as a prompt

Educating pupils about AI

Here at Isbourne Valley School we acknowledge that pupils benefit from a knowledge-rich curriculum that allows them to become well-informed users of technology and understand its impact on society. Strong foundational knowledge will ensure that pupils develop the right skills to make the best use of generative AI. Pupils are taught about the potential benefits of using AI tools to aid their learning, while also covering subjects such as:

- creating and using digital content safely and responsibly
- the limitations, reliability and potential bias of generative AI
- how information on the internet is organised and ranked
- online safety to protect against harmful or misleading content

Use of AI by pupils

We recognise that AI has many uses to help pupils learn. Pupils may use AI tools, for example, as a research tool to help them find out about new topics and ideas or when specifically studying and discussing AI in schoolwork, for example in IT lessons or art homework about AI-generated images.

All AI-generated content must be properly attributed and appropriate for the pupils' age and educational needs. AI may also lend itself to cheating and plagiarism. To mitigate this, pupils may not use AI tools during assessments, to write their homework or class assignments, where AI-generated text is presented as their own work, to complete their homework, where AI is used to answer questions and is presented as their own work (for example, maths calculations) - this list of AI misuse is not exhaustive.

Where AI tools have been used as a source of information, pupils should reference their use of AI. The reference must show the name of the AI source and the date the content was generated.

Pupils must consider what is ethical and appropriate in their use of AI and must not:

- generate content to impersonate, bully or harass another person
- generate (including by digitally altering) or share explicit or offensive content, including, but not limited to, inappropriate or sexualised images of themselves or other people (known as 'deepfakes' or 'deep nudes')
- input offensive, discriminatory or inappropriate content as a prompt

Formal assessments

We will continue to take reasonable steps where applicable to prevent malpractice involving the use of generative AI in assessments.

We will follow the latest guidance published by the Joint Council for Qualifications (JCQ) on [AI use in assessments](#).

Staff training

AI is a new and evolving concept and facility. We will assist staff in keeping up to date with developments in this area, utilising CPD and training opportunities, sharing best practice and in developing and improving their own practice.

Acceptable use of the internet in school

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

More information is set out in the acceptable use agreements in appendices 1 to 3.

Safeguarding concerns relating to the use of AI

We are aware that the use of generative AI may in some circumstances lead to safeguarding concerns including, but not limited to:

- Sexual grooming
- Sexual harassment
- Sexual extortion
- Child sexual abuse/exploitation material
- Harmful content
- Harmful advertisements and promotions
- Bullying

Where there are safeguarding concerns arising from the use of generative AI, a report must be made to the DSL immediately. Any such incident will be dealt with according to the procedures set out in our safeguarding policy, and any applicable child protection referral process.

Pupils using mobile devices in school

In line with statutory guidance, our school is a mobile phone-free environment by default. Pupils are not permitted to have access to or use their mobile phones or smart technology with similar functionality to mobile phones (e.g. smart watches), which we refer to collectively as 'mobile phones', throughout the school day. This prohibition includes all lessons, the time between lessons, breaktimes, and lunchtimes.

Any deviation from this mobile phone-free baseline will be by exception only (for example, approved arrangements for specific medical tracking or documented safeguarding needs) and must be explicitly authorised by the Headteacher.

Where there is an arrangement by exception, any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2). Any breach of the acceptable use agreement by a pupil may trigger a sanction in line with the school's behaviour policy, which may result in the confiscation of their device.

Staff using work devices outside school

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

- keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol);
- not sharing their passwords;
- making sure their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device;
- making sure the device locks if left inactive for a period of time;
- not sharing the device among family or friends;
- installing anti-virus and anti-spyware software; and
- keeping operating systems up to date by always installing the latest updates.

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

If staff have any concerns over the security of their device, they must seek advice from the ICT manager and/or Headteacher.

How the school will respond to issues of misuse

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

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

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

Breach of this policy

By staff

Breach of this policy by staff will be dealt with in line with our staff code of conduct. Where disciplinary action is appropriate, it may be taken whether the breach occurs:

- During or outside of working hours
- On an individual's own device or a school device
- At home, at school or from a remote working location

Staff members will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

- The generative AI application in question (whether or not it is one authorised by the school)
- Any relevant passwords or login details

All staff must report any breach of this policy, either by themselves or by another member of staff, to the Headteacher immediately.

By governors

Breach of this policy by governors will be investigated by the Headteacher, Chair of Governors, DPO or Network Manager as appropriate. Governors will be required to co-operate with any investigation into a suspected breach of this policy. This may involve providing us with access to:

- The generative AI application in question (whether or not it is one authorised by the school)
- Any relevant passwords or login details

A decision on the appropriate response, including action to be taken, will be made by a panel including the Headteacher, Network Manager, Chair of Governors and DPO.

By pupils

Any breach of this policy by a pupil will be dealt with in line with our behaviour and anti-bullying policies.

Monitoring arrangements

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

AI technology, and the benefits, risks and harms related to it, evolves and changes rapidly. Consequently, in this regard, this policy is a live document that must be kept updated by the Teaching & Learning Committee in response to guidance from the Headteacher, Network Manager or Online Safety Lead whenever there is a significant change to either AI use by the school or the associated risks of AI usage.

This policy will also be regularly reviewed by the Teaching & Learning Committee and updated annually to align with emerging best practices, technological advancements and changes in regulations. The review (such as the one available [here](#)) will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

The policy will be shared with the full governing body at least annually.

We will keep members of the school community up to date on the use of AI technologies for educational purposes. As part of our regular surveys, feedback from pupils, parents/carers and staff will be considered in the ongoing evaluation and development of AI use in school.

Links with other policies

This Online Safety policy works alongside and should be read in conjunction with the following other policies and documents:

Safeguarding

Behaviour

Anti-Bullying

Staff Discipline and Grievance

Staff Code of Conduct

Data protection

Privacy notices

Complaints

Equality and diversity

Appropriate use of mobile phones

Home Learning

Marking and Feedback

Adopted by Isbourne Valley School Governing Body 9th September 2026

Next review Autumn Term 2027

Appendix 1

EYFS and KS1 acceptable use guidance (pupils and parents/carers)

This appendix sets out our expectations for pupils and their parents and carers whilst pupils are in Coln and Avon classes (EYFS and KS1). We treat these expectations as part of our school rules and may apply consequences and sanctions if they are not followed.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

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

Appendix 2

KS2 acceptable use guidance (pupils and parents/carers)

This appendix sets out our expectations for pupils and their parents and carers whilst pupils are in Windrush and Evenlode classes (KS2). We treat these expectations as part of our school rules and may apply consequences and sanctions if they are not followed.

I will read and follow these rules.

When I use the school's ICT systems (like computers) and get onto the internet in school I will:

- Always use the school's ICT systems and the internet responsibly and for educational purposes only
- Only use them when a teacher is present, or with a teacher's permission
- Keep my usernames and passwords safe and not share these with others
- Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer
- Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others
- Only use generative AI in accordance with the school's Online Safety Policy
- Always log off or shut down a computer when I've finished working on it

I will not:

- Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate, including anything created using AI
- Log in to the school's network using someone else's details
- Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision

I will not bring a personal mobile phone or other personal electronic device into school unless the Headteacher has said that I can, and if I do I:

- will make sure it's switched off and handed to the school office as required by school rules immediately upon entering the school
- understand that I am not permitted to look at, use, or have access to my device at any point during the school day – including during lessons, the time between lessons, breaktimes, and lunchtimes
- will only use my device if I have official written permission from the school
- agree that if I break the school rules on mobile devices, my device will be confiscated

I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.

Appendix 3

Acceptable use agreement (staff, governors, volunteers and visitors)

This appendix sets out our expectations for staff, governors, volunteers and visitors. We treat these expectations as requirements and, as appropriate, in accordance with our codes of conduct and staffing disciplinary documents, procedures and processes.

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way that could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Input, upload, or process any personal data of pupils, confidential safeguarding information, or sensitive school data into public or unvetted generative AI tools (such as public AI chatbots or image generators). I will make sure I am aware of approved AI tools for use in school and follow this at all times
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me they have found any material that might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and will make sure that the pupils in my care also do so.

I will use generative AI in line with this Online Safety Policy.

Appendix 4
Online safety training needs – self-audit for staff

Name of staff member/volunteer:	Date:
Question	Yes/No (add comments if necessary)
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 5
online safety incident report log

Date	Where the incident took place	Description of the incident	Action taken	Name and signature of staff member recording the incident

Appendix 6

Approved uses of AI tools (table)

Note that open-source AI tools / open AI tools, meaning tools that anyone can access and modify, should only be used for tasks that don't require personal information to be input.

APPROVED AI TOOLS	APPROVED FOR	APPROVED USES
KeyGPT	• Teachers • Governors • Teaching Assistants • Administrative Assistants	• Letter to parents/carers • Job descriptions and adverts • Interview questions
Oak Academy AI lesson planner	• Teachers	Lesson planning