Woodstock CE Primary

Hand in hand we...
Love | Learn | Flourish

Policy for:

Online Safety

		Date
Reviewed by:	Staff & SLT	March 2026
Authorised by:	Resources	
Date for next review: (or earlier should legislation require it)	Autumn 2027	

Change Log	

Online Safety Policy

Aims of the Policy

We appreciate family life beyond school can be busy for most of us. We have reviewed our Homework Policy to

Our School Aims to:

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

The 4 Key Categories of Risk

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

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

Legislation and Guidance

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

- Teaching Online Safety
- Meeting Digital and Technology Standards
- Preventing and Tackling Bullying and Cyber-bullying: Advice for Headteachers and School Staff
- Relationships and Sex Education (RSE) and Health Education
- Searching, Screening and Confiscation

It also refers to the DfE's guidance on Protecting Children from Radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also considers the National Curriculum Computing Programmes of Study.

Roles and Responsibilities

The Governing Body

- Overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
- Ensure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.
- Make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
- Co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
- Ensure that the school teaches pupils how to keep themselves and others safe, including online.

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

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

The governor who oversees online safety is Lynne Hammond (Chair).

All Governors will:

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

The Headteacher

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

The Designated Safeguarding Lead (DSL) (supported by the school's DDSLs)

Details of the school's Designated Safeguarding Lead (DSL), and Deputy DSLS, are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

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

- Supporting the headteacher in making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and make sure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly

- Working with the ICT Systems Lead to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT Systems Lead and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Making sure that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks pupils face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

The ICT Systems Lead (123ICT – with support of our SBM)

The ICT manager is responsible for:

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

This list is not intended to be exhaustive.

All Staff and Volunteers

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

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and making sure that pupils follow the school's terms on acceptable use
- Knowing that the SBM (supported by the DSL and ICT Systems Lead) is responsible for the filtering and monitoring systems and processes, and being aware that the school uses Securus for filtering and monitoring. Any alerts or incidents triggered through the system are reviewed by the SBM, who will notify the appropriate person where necessary. Staff can also report any suspected misuse of systems by pupils directly to the SBM for further action.
- Following the correct procedures by seeking approval from the SBM and Headteacher, and then contacting 123ICT, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged (MyConcern) and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

Parents/Carers

Parents/carers are expected to:

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

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

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

Visitors and Members of the Community

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

Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum, as outlined in the **National Curriculum Computing Programmes of Study** and the government's **guidance on Relationships Education, Relationships and Sex Education (RSE) and Health Education (2026)**.

All schools must teach:

- Relationships Education and Health Education in primary schools

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

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

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 (currently 13), 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

The safe use of social media and the internet will also be covered in other subjects where relevant, including the annual celebration of Safer Internet Day, as well as within our broader curriculum, Computing and PSHE/RSHE. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Pupils will be taught practical cyber security skills

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 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 cyberbullying and the risks of online radicalisation.

Educating Parents/Carers about Online Safety

The school will raise parents/carers' awareness of internet safety in newsletters or other communications home, and in information via our website. This policy will also be shared with parents/carers. Online safety will also be covered during planned parents' workshops and relevant parent notifications.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use (through AUP)
- What their children are being asked to do online (Curriculum Maps and Long-term Plans)

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL. Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

Preventing and Addressing Cyber-Bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with class during planned PSHE/RSHE and Computing sessions in an age-appropriate manner.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.
The school also sends information via our newsletter 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 school 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 any incidents will 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

Our school has a no phones policy therefore the risk of in-school incidents is minimised. This also includes any other devices such as smart watches.

The Headteacher, and any member of staff authorised to do so by the headteacher (DSL & DDSLs, 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:

- Assess 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 or DSL/DDSLs.
- Explain to the pupil why they are being searched, and 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 the Senior Leadership Team (DSL/DDSLs) 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 whether 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/carer 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), they will:

- **Not** view the image

- 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**

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**
- 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 complaints procedure.

Artificial Intelligence (AI)

Pupil Use of Generative AI

Pupils at Woodstock CE Primary School do **not use open-access generative AI tools in school**.
The school does not expect pupils to create accounts for, directly access or independently interact with generative AI chatbots or similar open-access services as part of their learning.

This position reflects the age of our pupils, the age restrictions applied by many AI providers and our responsibility to ensure that technology used within school is safe, appropriate and educationally beneficial.

Should the school consider introducing any pupil-facing AI technology in the future, this would only take place following appropriate consideration of:

- safeguarding and online safety;
- age restrictions and terms of use;
- data protection and privacy;
- filtering and monitoring;
- the educational purpose and benefit of the technology;
- accessibility, equality and SEND;
- potential bias, misinformation and inappropriate content;
- intellectual property and copyright;
- the impact upon children's learning and cognitive, social and emotional development; and
- appropriate staff supervision and risk assessment.

Educating Children About AI

Although pupils do not use generative AI tools in school, we recognise that children are growing up in a world in which AI is increasingly common. Children may encounter AI-generated material through search engines, social media, gaming, video platforms, advertising and other online content outside school.

We therefore believe that **not using AI is different from not learning about AI**.

As part of our Computing, PSHE/RSHE and wider online safety curriculum, pupils will receive age-appropriate opportunities to develop their understanding of AI and the increasingly important skills needed to navigate AI-generated content safely.

As appropriate to their age and stage of development, children will be helped to understand:

- what AI is and some of the ways in which it is already used in everyday life;
- that computers and AI systems do not "think" or understand information in the same way that people do;
- that AI-generated information can be inaccurate, misleading, biased, inappropriate or entirely fabricated;
- that something which looks or sounds convincing online is not necessarily true;
- the importance of checking information against reliable sources and asking a trusted adult when unsure;
- that AI can be used to create or manipulate realistic-looking photographs, videos and audio, sometimes referred to as **deepfakes**;
- that images, voices and identities can be copied or manipulated using technology;

- that personal information, photographs or other people's work should not be entered into online tools without appropriate permission;
- the importance of copyright, ownership and acknowledging where information and ideas have come from; and
- how to report anything encountered online that worries, frightens, confuses or upsets them.

This education will form part of our wider commitment to developing children's **digital literacy and critical thinking**, helping pupils to question what they see online rather than automatically accepting digital content as accurate or genuine.

Safeguarding Risks Associated with AI

The school recognises that AI can create or increase existing online safety risks. These may include:

- misinformation and disinformation;
- convincing but false information;
- inappropriate, harmful or age-inappropriate content;
- deepfake images, audio or video;
- AI-generated sexual or abusive imagery;
- impersonation of pupils, staff or other individuals;
- cyberbullying and harassment;
- scams, phishing and manipulation;
- bias and discrimination;
- breaches of privacy or confidentiality; and
- inappropriate collection or use of personal data.

Any safeguarding concern involving AI will be treated in the same way as any other safeguarding or online safety concern and must be reported to the Designated Safeguarding Lead (DSL) or Deputy DSL immediately, in accordance with the school's Child Protection and Safeguarding Policy.

Where AI-generated material is used to bully, humiliate, impersonate, exploit or otherwise cause harm to another person, the school will respond in accordance with its safeguarding, behaviour, anti-bullying and online safety procedures. Where appropriate, external agencies, including the police, may be contacted.

Staff Use of Artificial Intelligence

Staff may have **limited and appropriate access to approved AI tools** where there is a clear professional or educational purpose. This may include supporting the creation or development of:

- teaching and learning resources;
- lesson ideas and activities;
- questions and quizzes;
- curriculum materials;
- administrative content; and
- other appropriate professional resources.

AI should be regarded as a tool to support professional practice and **not as a replacement for professional knowledge, judgement or accountability**.

Staff remain responsible for anything they create, adapt, communicate or use professionally, regardless of whether AI assisted in its production.

Staff must therefore critically review AI-generated material before it is used. This includes checking its accuracy, suitability, quality, bias, language, curriculum relevance, copyright implications and appropriateness for the age and needs of the children.

AI-generated content must never be assumed to be factually correct simply because it appears authoritative or convincing.

Protecting Personal and Safeguarding Information

Staff must take particular care when using generative AI because information entered into an AI system may be processed, stored or used by the provider.

Unless an AI system has been specifically approved by the school for processing such information, staff **must not enter personal, confidential or sensitive information into generative AI tools**.

This includes, but is not limited to:

- pupils' names or information that could identify an individual pupil;
- photographs or images of pupils;
- personal information about pupils, parents/carers or staff;
- safeguarding information;
- information from MyConcern or safeguarding records;
- SEND information;
- medical information;
- behaviour records;
- assessment information linked to identifiable pupils; or
- confidential school, personnel or family information.

Information must not simply be anonymised by replacing a child's name if the remaining information could still enable that child or family to be identified. Staff must follow the school's Data Protection Policy and seek advice from SBM/ Data Protection Officer where they are unsure.

Human Oversight and Professional Responsibility

AI will not make safeguarding decisions on behalf of the school.

AI must not be relied upon to determine whether a child is at risk, interpret safeguarding information, decide whether a referral should be made, determine sanctions or make other significant decisions about an individual child.

Such decisions require professional judgement, knowledge of the child and their circumstances, and the school's established safeguarding and decision-making procedures.
AI will similarly not replace teachers' professional assessment of children's learning, progress or individual needs.

Approval and Risk Assessment of AI Tools

The introduction of new AI tools or significant new uses of existing AI technology must be appropriately considered before implementation.

Where relevant, the school will consider:

- the purpose and educational benefit of the tool;
- the age of intended users;
- safeguarding implications;
- data protection and privacy;
- how information entered into the system is stored or used;
- filtering and monitoring requirements;
- cyber security;
- intellectual property and copyright;
- bias, equality and accessibility;
- whether a Data Protection Impact Assessment (DPIA) is required; and
- whether appropriate staff training is required.

Staff should not independently introduce AI systems for use with pupils without appropriate school approval.

Staff Training and Awareness

The school recognises that AI technology and associated risks are developing rapidly.

Staff will therefore receive appropriate information, guidance and training to ensure they understand:

- the school's expectations regarding AI;
- appropriate and inappropriate uses of generative AI;
- safeguarding risks associated with AI;
- data protection and confidentiality;
- misinformation, bias and AI "hallucinations";
- deepfakes and manipulated content;
- copyright and intellectual property considerations; and
- their continuing professional responsibility for material produced with the assistance of AI.

AI will be considered as part of the school's wider online safety and safeguarding training and updates.

Working with Parents and Carers

The school recognises the important role parents and carers play in helping children understand new technologies.

Where appropriate, the school will provide information to parents/carers about emerging AI risks and the ways in which children may encounter AI outside school.

Parents/carers are encouraged to be aware of age restrictions attached to AI platforms, talk to their children about AI-generated content, encourage children to question whether online information is reliable and ensure children know that they should speak to a trusted adult if something online worries or confuses them.

Governance and Review

The Governing Body will maintain appropriate oversight of the school's approach to AI as part of its wider responsibilities for safeguarding, online safety, data protection and the school's digital strategy.

The school will keep its approach to AI under review because the technology, associated risks and national guidance continue to develop rapidly.

This section should therefore be read alongside the school's:

- Child Protection and Safeguarding Policy;
- Data Protection Policy and Privacy Notices;
- ICT and Internet Acceptable Use Policy;
- Staff Code of Conduct;
- Behaviour Policy;
- Anti-Bullying and Anti-Cyber Bullying Policy;
- PSHE/RSHE Policy; and
- any separate AI Usage Policy adopted by the school.

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. 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 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.

Pupils Using Mobile Devices in School

Children are not allowed to bring any mobile devices into school. If a mobile device in needed, for example, in the case of a Year 6 pupil who walks home from school, an agreement is made with parents of the child, the mobile device is locked in the teacher's drawer and returned at the end of the school day.

Any misuse of this agreed system will result in no mobile device being allowed to be brought in by the child.

Staff Using Work Devices Outside School

All staff members will take appropriate steps to ensure their devices remain secure – this has been supported by our IT Tech Lead (123ICT), who ensure the following is well maintained. This includes, but is not limited to:

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

Staff members must not use the device in any way that would violate the school's terms of acceptable use. 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 School's Business Manager who will work with our IT Tech Lead.

How the School will Respond to Issues of Misuse

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

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Procedures / Staff Code of Conduct]. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Training for Staff, Governors and Volunteers

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation (this is part of the Keeping Children Safe in Education updates Generalist Training and annual updates).

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

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

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- 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 ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL (or DDSLs) will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually. Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our child protection and safeguarding policy.

Monitoring Arrangements

The DSL logs behaviour and safeguarding issues related to online safety on our MyConcern Safeguarding system. This policy will be reviewed annually the DSL/SBM. At every review, the policy will be shared with the governing board. The review will be supported by an annual risk assessment that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Keeping Children Safe in Education
- Behaviour Policy
- Staff Disciplinary Procedures/ Staff Code of Conduct
- Data Protection Policy and Privacy Notices
- Complaints Procedure
- ICT and Internet Acceptable Use Policy
- PSHE/RSHE Policy
- Anti-Bullying & Anti-Cyber Bullying Policy