ONLINE SAFETY POLICY

Introduction

This policy is focussed on the knowledge and behaviours that will help students and staff to safely benefit from the online world, regardless of the device, platform or app that is used. Specific guidance is available separately (for example an Acceptable Use Agreement) and this will be regularly reviewed in the light of technological changes and experience. This policy builds on the requirements of 'Keeping Children Safe in Education' and information of where the main sources of guidance can be found are at the end of this policy.

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

Roles and responsibilities

The governing board

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

The governing board will make sure 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.

The governing board will also 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.

The governing board will 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).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure 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 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 their safeguarding needs

All governors will:

- Ensure 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
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure 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 ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The Headtecaher should assign a member of the SLT to be the digital online safety lead.

The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

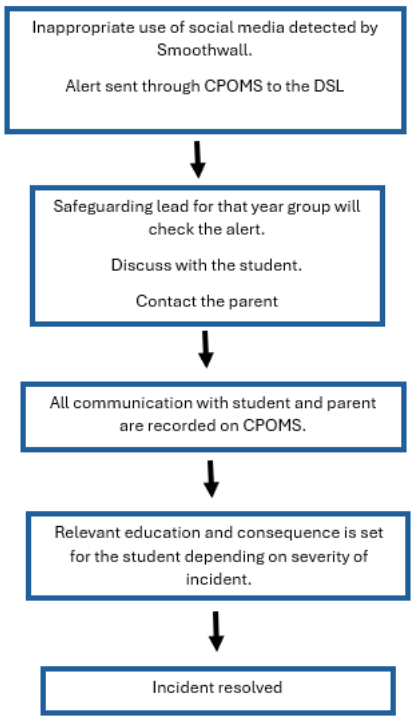
The DSL Emma Tindall, takes lead responsibility for online safety in school and is the digital lead for the school. The Assistant Head Mark Tucker leads the school development in the use of AI technology.

- The DSL will have strategic oversight of all digital technology and how it fits with their development plan and create and manage the digital technology strategy led by the needs of staff and students, not the technology itself.
- The DSL will lead the online safety team that will include:
    - The safeguarding team
    - IT technical team
    - Curriculum lead for IT
    - The data protection officer
    - The HR manager

- The DSL will help all staff to embed digital technology that meets staff and student needs

- Supporting the Headteacher in ensuring 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
- Taking the lead on 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 Child protection and safeguarding policy.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy. Online safety concerns that are raised through SENSO are filtered and then recorded on CPOMS and followed up with all students and parents.

Online incident follow up procedure:



- Ensuring 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 children 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

The ICT manager

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 ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring 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 regular basis.
- Review the filtering and monitoring provision at least annually.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- They have an awareness of new technologies that reduce the effectiveness of filtering measures.

- Ensure that all new staff and students agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

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 ensuring, that pupils follow the school's terms on acceptable use.
- 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.
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes by contacting the IT team directly.
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- 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'
- All staff using IT systems within their classroom use **in-person monitoring throughout** their lesson to monitor the use of the computers and online systems**.** Staff should report to the DSL team if they have any concerns about students use of the school online system and record on CPOMS.
- Staff should not be using their personal mobile devices, smart watches and tablets during the school day within registration, lesson time or when around the school site, including when on duty. Personal devices should only be used when in staff office spaces and not around students. If any staff member if concerns about the way a member of staff is using their mobile or smart devices when on the school premises, then they should be reported to the Headteacher and a record on CPOMS staff safe. If concerns are raised in relation to a visitor on site this should be reported directly to the DSL or Headteacher.
- Staff should never use a personal mobile device, tablet or smart watch when in the PE changing rooms.
- Ensure that any devices that are bought in from home (BYOD) have adequate filtering and monitoring measures in place and that these are monitored by the IT team.

Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concern or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.

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
- Childnet - Parent resource sheet and hot topics – Childnet — Online safety for young people
- Keeping children safe online | NSPCC

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.

Learning for safety

The school will ensure that students and staff understand how to use online school systems safely and that this knowledge is regularly updated. For staff this will be through regular staff training and for students it will be through the taught curriculum (Relationships and Sex Education, Health Education, Computing and other subjects) together with the broader curriculum (Safeguarding, guidance and opportunities such as assemblies). Where appropriate, the latter will be supported by activities for students' families.

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, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism. This category explicitly includes misinformation, disinformation and conspiracy theories.

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 them 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; and

Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Knowledge and Behaviours

There are five key outcomes that the online curriculum will help students achieve. These combine developing knowledge with an understanding of the student's behaviour and that of others, both on and offline.

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- How to **evaluate what they see online** – The ability to make judgements about what they see and to ask themselves whether it is: Fact or opinion? Too good to be true? Fake or genuine? Fair? Acceptable?
- How to recognise when approaches are being used to **convince them to think or respond in a particular way**. To continue gaming, to buy something or to spread false information
- To **recognise and practice acceptable online behaviour** - A high standard of behaviour and honesty is expected both online and offline. This includes understanding the effects of online anonymity, how peer pressure intensifies emotions and techniques to deal with conflict and negative language. To behave appropriately during remote learning, with regard to working and communicating with the teacher and other students
- How to **identify online risks** – Having the knowledge of a range of online risks to recognise these behaviours and then decide on the best course of action. This requires the development of judgement in respect of sharing personal information, when to participate in an activity and that a digital footprint can be viewed many years in the future

How and when to seek support and report concerns

- Who to turn to if they are concerned or upset by something they have seen online. To know the adults they can trust, as well as knowing how to access support from school staff and organisations such as the police, Childline and CEOP. They should also know that platforms and apps will have ways in which inappropriate contact or content can be reported
- To understand when to report concerns around mobile phone use by adults to the safeguarding team. This can include their Head of year or one of the DSL team.
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Risks

The students' learning about online safety will develop knowledge and skills to ensure they enjoy safe and positive experiences online. The rapidly changing nature of online technology means that risks will change and the following highlights the main areas of risk considered by the whole curriculum.

Using the internet and the information it contains:

- Age restrictions to protect young people
- How content can be used and shared
- Disinformation, misinformation and hoaxes
- Fake websites and scam emails
- Online fraud
- Password phishing
- Gathering personal data

- Persuasive design
- Privacy settings
- Targeting of online content

Staying safe online:

- Online abuse
- Online challenges
- Content that incites – hatred or violence
- Fake profiles
- Grooming
- Live streaming a video, usually of yourself
- Pornography
- Communicating with people you have not met

Wellbeing:

- Impact on confidence, particularly body image
- Impact on physical and mental health
- People behaving differently online and offline
- Long-term reputational damage
- Highlighting of self-harm and eating disorders

Within any group of students or staff, some will have personal experience of the impact of these risks. Others may be particularly susceptible to online harm or have less support from family or friends. The school will be proactive in ensuring all who may be potentially affected in this way, receive the information and support they need. This will be achieved through good communication between staff and the maintenance of a highly positive Safeguarding environment in which all feel supported in raising issues.

Educating parents/carers about online safety

The school will raise parents/carers' awareness of internet safety in letters 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 parents information evenings.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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.

Preventing and addressing cyber-bullying

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

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.

The school also sends 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 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 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.

Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Warlingham School recognises 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.

Warlingham School will treat any use of AI to bully pupils in line with our anti-bullying and behaviour policy and our Child protection and Safeguarding policy.

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 by the school.

Network Security - Filters and Monitoring

As part of the school's work to reduce online risks, it has in place a range of filters and monitoring system called SENSO The choice of appropriate tools has been informed by a risk assessment that reflects the age and experience of our students. While online safety is the main priority, a balance will be maintained between safety, use of resources and the dangers of 'over blocking'. Mobile technology presents challenges for network security both at school and at home. The knowledge and skills gained through the curriculum will help students keep themselves safe online when using mobile technology outside of school. However, families must ensure that comparable filtering systems are in place to support students at home.

Staff Training

All new staff members will receive training as part of their induction on online safety (including grooming, cyber-bullying and the risks of online radicalisation). All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates through emails, bulletins and staff meetings. The Designated Safeguarding Lead and deputies will undertake child protection and safeguarding training, including 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. Users will also be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss.

Monitoring and Review

Records of any online safety incidents will be kept by the Safeguarding or IT teams as appropriate. These will be reviewed by the responsible member of the Senior Leadership Team as necessary and at least termly. They will also be responsible for providing Governors with summary information to enable them to make a judgement about the fitness for purpose of this policy at the time of review.

Acceptable use of the internet in school

All students, parents, staff, volunteers and governors that are part of our community are expected to uphold and work in line with our acceptable use of the school's ICT systems and the internet agreement. 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 the individual's role. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Pupils using mobile devices in school

Pupils are permitted to bring mobile phones into school to support them with their journey to and from school. Year 7 are not allowed to have a smart phone on them in school. Year 8-11 students must hand their smart phones in at the morning line up and this is placed in the lock box for the day. This is then returned to the students when they leave the school site.

Students are able to contact home from student services during the school day.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device for a minimum of 5 days. Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on [behaviour and ICT and internet acceptable use and the action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Examining electronic devices

School staff will not search students phones. If a student has an online issue that they would like to share with their Head of year then they should come to the Reflection room and the member of staff will investigate with the students permission which may include the student showing messages form their phone. This would only happen if the student has given consent and the sharing information has been documented.

If a student has used their mobile phone inappropriately on the school site then a member of the SLT or safeguarding team, are able to request the student deletes any images or messages. When deciding whether there is a good reason a student should erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police

Staff using work devices outside school

All staff members will take appropriate steps to ensure 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)
- 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 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.
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 IT manager.

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 and LADO.

Please also refer to:

DFE Teaching online safety in school 2023

Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK

Keeping Children Safe in Education (KCSIE) 2024

DFE Relationships and Sex Education, and Health Education 2026

DfE Searching, screening and confiscation

DfE Protecting children from radicalisation

DfE Preventing and tackling bullying and cyber-bullying

Online safety section of keeping children safe in education, paragraphs 123-135

Safer internet centre

UK Council for Internet Safety (UKCIS)

Online safety self-review tool for schools

Broadband internet standards for schools and colleges

Digital leadership and governance standards

Filtering and monitoring standards for schools and colleges

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 students' 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.

This Policy should be read in conjunction with the following policies:

- Anti-bullying Policy
- Behaviour for Learning Policy
- Child Protection and Safeguarding Policy
- Code of Conduct and Staff Behaviour Policy
- ICT Use and Online Safety Policy
- Mobile Phone Policy

Approved by Local Governing Body	Spring 2026
Due for review	Spring 2027
SLT Member	Mrs K Haynes and Ms E Tindall