MANOR GREEN SCHOOL

Excellence for All

ONLINE SAFETY POLICY OCTOBER 2025

Rationale

Manor Green understands that using online services is an important aspect of raising educational standards, promoting student achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of students and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect students and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

Legal Framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2025) ‘Filtering and monitoring standards for schools and colleges’
- DfE (2021) ‘Harmful online challenges and online hoaxes’
- DfE (2025) ‘Keeping children safe in education September 2025’
- DfE (2023) ‘Teaching online safety in school’
- DfE (2023) ‘Searching, screening and confiscation’
- DfE (2025) ‘Generative artificial intelligence in education’

- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2024) ‘Sharing nudes and semi-nudes: advice for education settings working with children and young people’
- UK Council for Child Internet Safety (2020) ‘Education for a Connected World – 2020 edition’
- National Cyber Security Centre (2020) ‘Small Business Guide: Cyber Security’

This policy operates in conjunction with the following school policies:

- Anti-bullying Policy
- Behaviour Support Policy
- Communication Policy
- Curriculum Policy
- Equal Opportunities Policy (Students)
- Health and Safety Policy
- Home Learning Policy
- Children Looked After Policy
- Nurture Policy
- Relationships and Sex Education Policy
- Remote Learning Policy
- Remote Learning and Education: Information for Parents
- Safeguarding Policy
- Safer Recruitment and DBS Policy
- Social Media Policy
- UK GDPR (Data Protection) Policy
-

Roles and Responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL’s remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Headteacher is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an annual basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSLs by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping students safe.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Keeping up to date with current research, legislation and online trends.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Working with the Head Teacher and governing board to update this policy on an annual basis.
- Carrying out an annual safety audit of the school's on-line safety procedures

The ICT Manager is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated and maintained as appropriate and that any flagged concerns are reported to the DSL.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that students may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from the Headteacher and wider Leadership Team where appropriate and will ensure that there are strong processes in place to handle any concerns about students' safety online.

The importance of online safety is integrated across all school operations in the following ways:

- Staff receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum at a level and understanding relevant to our various cohorts.
- Parents are given relevant updates regarding online safety risks/trends

Handling online safety concerns:

Any disclosures made by students to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding Policy.

Concerns regarding a staff member's online behaviour are reported to the Headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the Headteacher, it is reported to the chair of governors.

Concerns regarding a student's online behaviour are reported to the DSL, who investigates concerns with relevant staff members and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Support Policy or Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Headteacher or DSL will contact the Police. The school avoids unnecessarily criminalising students, e.g. calling the Police where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and shared a nude picture with another student. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding Policy.
All online safety incidents and the school's response are recorded by the DSL.

Mental Health

The internet, particularly social media, can be the root cause of a number of mental health issues in students, e.g. low self-esteem and suicidal ideation. Staff will be aware that online activity both in and outside of school can have a substantial impact on a student's mental state, both positively and negatively.

The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a student is suffering from challenges in their mental health.

Online hoax/ Disinformation, Harmful online challenges, Misinformation and Conspiracy Theories

For the purposes of this policy, an **"online hoax"** or **"disinformation"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger, deceive or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same.

For the purposes of this policy, **"misinformation"** refers to false information spread accidentally or without malicious intent usually occurring due to a misunderstanding or genuine mistake.

For the purposes of this policy, **"conspiracy theories"** refers to a belief that events are secretly manipulated by powerful forces with negative intentions.

Online content/information becomes harmful when it puts the student at risk of harm, due to it negatively influencing a student's beliefs, behaviours and wellbeing.

Where staff suspect there may be a harmful online content being circulating amongst students in the school, they will report this to the DSL immediately. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to students, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.

Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing students.
- Not inadvertently encouraging students to view the content where they would not have otherwise come across it, e.g. where content is explained to younger students but is almost exclusively being shared amongst older students.
- Proportional to the actual or perceived risk.
- Helpful to the students who are, or are perceived to be, at risk.
- Appropriate for the relevant students' age and developmental stage.
- Supportive.

- In line with the Safeguarding Policy.

Cyber-Crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled –** these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'DDOS Attack', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that students with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a student's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Headteacher will ensure that students are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that students cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that students are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and Safeguarding Policy.

Online safety and the curriculum

Online safety is embedded throughout the curriculum and its teaching is always appropriate to students' ages and developmental stages.

Students are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours students learn through the curriculum include the following:

- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks and fake news

- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks students may face online are always considered when developing the curriculum.
The DSL is involved with the development of the school's online safety curriculum. Students will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online. Relevant members of staff work together to ensure the curriculum is tailored so these students receive the information and support they need.

The school will also endeavor to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from students.

Class teachers review external resources prior to using them for their curriculum, to ensure they are appropriate for the cohort of students. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they appropriate for students' developmental stage?

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

During a lesson or activity, the class teacher ensures a safe environment is maintained in which students feel comfortable to say what they feel and ask questions and are not worried about getting into trouble or being judged. If a staff member is concerned about anything students raise during lessons and activities, they will make a report in line with the Safeguarding Policy.

Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Laptops
- Tablets
- Internet
- Email
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Students are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

Mobile Phones

Students are allowed to bring mobile phones into school as many of our students will use them during their travel to and from school. However, once school starts all phones must be handed in to class staff and will be locked away in a secure location until the end of the school day.

Educating Parents

The school works in partnership with parents to ensure students stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of students, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content, via Online resources, direct support from staff, and parent emails

Filtering and monitoring online activity

The Headteacher and ICT Manager ensure the school's ICT network has appropriate filters and monitoring systems in place whilst, at the same time, ensuring 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

The Headteacher and ICT Manager undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks.

The ICT Manager undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate. Requests regarding making changes to the filtering system are directed to the ICT Manager or Headteacher and prior to making any changes to the filtering system, a risk assessment is carried out. All requests are logged and reviewed regularly to see if they are still relevant.

Any changes made to the system are recorded by the ICT Manager. Reports of inappropriate websites or materials are made to the ICT Manager immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and ICT Manager, who will escalate the matter appropriately. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation

(IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Safeguarding Policy.

Network Security:

Technical security features, such as anti-virus software, are kept up-to-date and managed by the ICT Manager. Firewalls are switched on at all times. The ICT Manager reviews the firewalls on a regular basis to ensure they are running correctly, and to carry out any required updates.

Staff and students are advised not to download unapproved software or open unfamiliar email attachments and are expected to report all malware and virus attacks to the ICT Manager.

All members of staff have their own unique usernames and private passwords to access the school's systems. Students, where appropriate, are provided with their own unique username and private passwords. Staff members and students are responsible for keeping their passwords private.

Users inform the ICT Manager if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. Users are required to lock access to devices and systems when they are not in use. Automatic screen lock is set up via Group Policy.

Emails

Staff and students are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and students are required to block spam and junk mail and report the matter to the ICT Manager. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and students are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

School Website

The Headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and students is not published on the website. Images and videos are only posted on the website if the relevant provisions are met.

Use of devices

School-owned devices

Some staff members are issued with the following devices to assist with their work:

- Laptop
- Tablet

- Desktop
- Mobile Phone

Students are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons. Staff and students are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected.

The ICT Manager will review all school-owned devices on a regular basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from the ICT Manager

Personal devices

Any personal electronic device that is brought into school is the responsibility of the user and staff members are not permitted to use their personal devices during lesson time, other than in an emergency. Staff members are not permitted to use their personal devices to take photos or videos of students.

If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Headteacher will inform the police, and action will be taken in line with the relevant policies.

Students' devices can be searched, screened and confiscated if a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence. Any concerns about use of personal devices on the school premises are reported to the DSL.

Raising Awareness of this Policy

We will raise awareness of this policy via:

- the school website
- the School Bus Compliance Manager
- the Staff Handbook
- meetings with parents
- school events
- meetings with school staff
- communications with home
- Headteacher's reports
- information displays in the main school entrance

Equality Impact Assessment

Under the Equality Act 2010 we have a duty not to discriminate against people based on their age, disability, gender reassignment, marriage or civil partnership, pregnancy or maternity, race, religion or belief, sex or sexual orientation.

This policy has been equality impact assessed, and we believe that it is in line with the Equality Act 2010. As it is fair, it does not prioritise or disadvantage any student, and it helps to promote equality at this school.

Monitoring the effectiveness of the policy

This procedure shall be subject to annual review.

The Governing Board approved this policy on date: 3rd July 2024

Signed: Richard Pelly, Chair of Governors

Signed: Joolz Scarlett, Head Teacher