Manor Green School: Online safety audit

Assessment conducted by: Warren Griffiths	Job title: Deputy Principal	Date of assessment: September 2026
Review interval: Six-monthly	Date of next review: April 27	

Risk rating		Likelihood of occurrence		
		Probable	**Possible**	**Remote**
Likely impact	**Major** Causes major physical injury, harm or ill health.	High (H)	H	Medium (M)
	Severe Causes physical injury or illness requiring first aid.	H	M	Low (L)
	Minor Causes physical or emotional discomfort.	M	L	L

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
1.Awareness of policies and procedures	H	• All staff are aware of all relevant policies and procedures including, but not limited to, the following:	Y	Head Teacher, ICT Manager,	Completed but functions	M

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
		○ Anti-bullying Policy ○ Behaviour Support Policy ○ Children Looked After Policy ○ Communication Policy ○ Curriculum Policy ○ Equal Opportunities Policy (Students) ○ Health and Safety Policy ○ Home Learning Policy ○ Nurture Policy ○ Online Safety Policy ○ PSHE and Relationships, Health 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 • Staff take responsibility for the security of ICT systems and electronic data they use or have access to. • Staff have an awareness of online safety issues and are familiar with, and understand, the signs that students may be unsafe online. • Staff report online safety concerns in line with the school's reporting procedure outlined in the Safeguarding Policy • Pupils are encouraged to report online safety concerns to their class staff or the Safeguarding Team		Deputy Principal, All Staff	need to be on going	

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
		• All staff are required to complete Annual Safeguarding Training, read Part One of Keeping Children Safe in Education, read the school Safeguarding Policy, and read the school Handbook all of which gives guidance and process around online safety and expected behaviours • The ICT Manager implements appropriate security measures and ensures that the school's filtering and monitoring systems (Smoothwall) are updated as appropriate.				
2.Managing online safety	H	• Staff are aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people. • The DSL has overall responsibility for the school's approach to online safety, with support from Deputy DSLs and ICT Manager where appropriate. • The importance of online safety is integrated across all school operations. • All staff receive safeguarding training (including online safety). • 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 across all departments. • Disclosures made by students to staff members about online abuse, harassment, risks or exploitation are handled in line with the Safeguarding Policy. • Concerns regarding a staff member's online behaviour are reported to the Head Teacher with consideration given as to whether a LADO referral is needed.	Y	Head Teacher, ICT Manager, Deputy Principal, All Staff	Completed but functions need to be on going	M

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
		• Concerns regarding a student's online behaviour are reported to the DSL or Deputy DSL, who investigate concerns using the Four C's Framework of online safety; Content, Contact, Conduct, and Commerce • Police and Social Care will be contacted if there is a concern that illegal activity has taken place. • All online safety incidents and the school's response are recorded by the DSL or relevant Deputy DSL on the school's safeguarding database; MyConcern				
3.Mental health	H	• Through training and briefings, staff are 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 ensures that, when necessary, training is available to ensure that staff members understand popular social media sites and terminology, how social media, AI and the internet can impact mental health, and the indicators that a student is suffering from challenges in their mental health. • The school has in place a comprehensive range of mental health interventions for students which can also be extended to parents/carers • Staff are encouraged to discuss mental health issues with their line manager and wider staff teams and the appropriate support is put in place. • Support for staff with mental health concerns is available via our Employee Assistance Programme, counselling and our Mental Health Champions	Y	Head Teacher, ICT Manager, Deputy Principal, All Staff	Completed but functions need to be on going	M

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
4.Online hoaxes, AI and harmful online challenges	H	• The DSL (and if necessary, ICT Manager) conducts a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils. • Where the assessment finds an online challenge, AI or hoax to be putting pupils at risk of harm, they ensure that the challenge is directly addressed with the relevant pupils. • A school-wide approach to highlighting potential harms of a hoax, AI or challenge is taken. • Controls are implemented to reduce the risk of potential harms of a hoax, AI or challenge including firewall (Smoothwall), anti-virus software and warning emails are sent out to inform staff.	Y	Head Teacher, ICT Manager, Deputy Principal	Completed but functions need to be on going	L
5.Online safety training for staff	M	• 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 are made aware that students are at risk of abuse by their peers and by adults, online as well as in person, and that abuse can take place concurrently via online channels and in daily life. • Staff are provided with ongoing updates and information (via email, signposting, school website) regarding online trends/risks and how to manage this	Y	Deputy Principal and ICT Manager	Always on going	L
6.Online safety and the curriculum	H	• Online safety is embedded throughout the curriculum (via PSHE/RSE) and is always appropriate to students' ages and developmental stages. • The school recognises that there are some pupils who may be more susceptible to online harm e.g. Children Looked After • Assistant Head Teachers work together with their respective Teachers to ensure the curriculum is tailored so their cohorts of	Y	Deputy Principal, Assistant Head Teachers, Deputy DSLs	Always on going	M

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
		students receive the information and support they need and addresses contextual topics. • During all lessons or activity, the Teachers ensures a safe environment is maintained in which students feel comfortable to say what they feel and ask questions. • We have a culture within the school where all safeguarding and wellbeing concerns are taken seriously and reported in a timely manner to the DSL or Deputy DSLs. • Any new curriculum content that is inaccessible due to filtering parameters must be submitted to the ICT Manager and DSL who will liaise with the department Assistant Headteacher to determine whether access should be allowed		and Class Teachers		
7.Use of technology in the classroom	M	• The teacher reviews and evaluates the resource prior to using any websites, tools, apps or other online platforms in the classroom. • Teachers ensure that any internet-derived materials are used in line with relevant legislation and policies e.g. copyright law. • Students are supervised when using online materials during lesson time and this supervision is suitable to their age and ability. • 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. • 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.	Y	All Staff and applicable students	Always on going	L

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
		• Staff and students are permitted to connect to personal Wi-Fi networks when working and learning from home. • All school-owned devices are password protected. • The ICT Manager reviews 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.				
8.Educating parents	M	• The school works in partnership with parents to ensure students stay safe online at school and at home. • Parents are made aware of the various ways in which their children may be at risk online. • Parents are 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.	Y	Relevant class staff, Parenting Worker, ICT Manager, DSL and Deputy DSLs	Always on going	L
9.Social networking	L	• Access to social networking sites is filtered as appropriate. • Staff and students are not permitted to use social media for personal use during lesson time. • Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. • Staff are not permitted to communicate with students or parents over social networking sites. • All communication on official social media channels by staff on behalf of the school is clear, transparent and open to scrutiny.	Y	All staff	Always on going	L
10.Network security	H	• Firewall is switched on at all times. • Staff and students are directed not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to the ICT Manager	Y	ICT Manager, all staff and relevant students	Always on going	M

Area for concern	Risk rating prior to action H/M/L	Recommended controls	In place? Yes/No	By whom?	Deadline	Risk rating following action H/M/L
		• All members of staff have their own unique usernames and private passwords to access the school's systems and where applicable students too. • 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.				
11.Filtering and monitoring online activity	H	• The school's ICT network has appropriate filters and monitoring systems in place ensuring that blocking does not restrict learning. • The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. • The ICT Manager regularly checks (weekly test) on the filtering and monitoring systems to ensure they are effective and appropriate. • Breaches of the filtering and monitoring system are automatically flagged to the DSL (Deputy Principal), Headteacher, Deputy Headteacher and ICT Manager. For every breach, the DSL will investigate and take the appropriate safeguarding action. Material that is believed to be illegal is accessed, inadvertently or deliberately, will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police. • Persistent breaches by students will inform necessary changes to online safety curriculum • The school's network and school-owned devices are appropriately monitored.	Y	ICT Manager, Deputy Principal	Always on going	M