Online Safety and Internet Use Policy

Date Policy due to be reviewed: September 2026

Committee Responsible for Policy: Full Academy Trust

WORK HARD | BE KIND | AIM HIGH

Section 1: Introduction

All schools must have regards to 'Keeping children safe in education' (September 2025) when carrying out their duties to safeguard and promote the welfare of children. At Hillcrest School staff, students, parents/carers and governors recognise that they exist in a world where technology is readily available to all. The school embraces the impact that such technology can have on a young person's social development, employability and technological competency. Nevertheless, Hillcrest School takes very seriously its responsibility for the 'Online Safety' of its community, and it is an integral aspect of our whole school approach to safeguarding and promoting British Values. We recognise that the abuse of technology, including malicious use of social media and the Internet, can have profound psychological and material consequences for victims of such abuse and therefore make every effort to ensure that safe use of technology is ensured within and outside of school.

In line with 'Teaching on-line safety in schools' (DFE – June 2019) and 'Meeting digital and technology standards in schools' (updated March 2023), Hillcrest School believes that the use of information and communication technologies (ICT) in school brings great benefits, including through the growing use of generative AI technology. New and smart technologies have become integral to the lives of young people today, both within schools and in their lives outside of school, as most have unrestricted access via 3G, 4G and 5G on phones, tablets and smart devices. The internet and other digital information and communications technologies are powerful tools, which open new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. However, young people always have an entitlement to safe internet access, and we recognise our duty to protect young people from different online risks, including ranging from the cyber-bullying, misinformation, disinformation, conspiracy theories, hate crime, child-on-child abuse, cybercrime, gambling, pornography and AI generated imagery, sexual harassment and threat of sexual exploitation, to involvement in gang activities and indoctrination from forms of extremist activities and organisations.

The statutory curriculum requires students to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and teach about the risks facing young people online, particularly in regard to AI technology and content. Computer skills are vital to access life-long learning and employment; indeed, ICT is now seen as an essential life-skill. Most technologies present risks as well as benefits. Internet use for work, home, social and leisure activities is expanding in all sectors of society. This brings young people into contact with a wide variety of influences, some of which – as in life generally – may be unsuitable.

This policy has been reviewed and updated in line with remote learning processes in school. Remote learning has inevitably led to a significant increase in the use of technology and online resources. As outlined in DFE guidance, we will continue to consider the safety of students if and/or when they are asked to work online at home or use school loaned technology to support their studies at home. This policy applies equally to existing or new online remote learning arrangements. In addition, keeping teachers safe when providing remote learning is integral to this policy.

WHAT IS ONLINE SAFETY?

Online Safety encompasses internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and parents/carers about the benefits and risks of using new technology, notably the growth in usage

of AI generated content, and provides safeguards and awareness for users to enable them to control their online experiences. The Schools' Online Safety Policy has been written to reflect the need to raise awareness of the safety issues associated with electronic communications. It also reflects the increased focus on online safety in Keeping Children Safe in Education (September 2025), DFE 'Generative AI: product safety expectations' (May 2025), 'Meeting digital and technology standards in schools and colleges (updated March 2023), Ofsted's review of sexual abuse in schools and colleges (April 2021) and 'Education for a connected world' (UK Council for Internet Safety - November 2020).

The purpose of this policy is to:

- Set out the key principles expected of all members of the school community at Hillcrest School with respect to the use of IT-based technologies.
- Safeguard and protect the children and staff.
- Assist school staff working with children to work safely and responsibly with the Internet and other IT and communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use for the whole school community.
- Have clear structures to for children to report and staff to deal with online abuse such as child-on-child abuse, inappropriate AI generated content, cyber-bullying, sexual harassment, criminal and sexual exploitation (noting that these need to be cross referenced with other school policies).
- Ensure that all members of the school community are aware of our zero-tolerance approach and that inappropriate, unlawful or unsafe online behaviour will be dealt with in accordance with our Behaviour and Anti-bullying policies.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.
- Set clear expectations for remote learning and live learning to ensure the safety of both staff and students.
- Promote the fundamental British Values in all forms of online activity.

The main areas of risk for our school community can be summarised as follows:

CONTENT

- Exposure to inappropriate and harmful content
- Lifestyle websites promoting harmful behaviours
- Hate content
- Misinformation, disinformation and conspiracy theories
- Content validation: how to check authenticity and accuracy of online content

CONTACT

- Grooming (sexual exploitation, radicalisation, extremism etc.)
- Online bullying in all forms
- Social or commercial identity theft and cybercrime, including passwords

CONDUCT

- Aggressive behaviours (bullying, harassment, violence, sexual/criminal exploitation)
- Privacy issues, including disclosure of personal information

- Digital footprint and online reputation
- Health and well-being (amount of time spent online, body image)
- Sexting (creating and circulation of nude and semi-nude images)
- Copyright (little care or consideration for intellectual property and ownership)

COMMERCE

- Online gambling
- Inappropriate advertising
- Phishing
- Financial scams

Section 2: Use of the Internet is important

The rapid developments in electronic communications are having many effects on society.

- The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and business administration systems.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.

Internet benefits for education

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- educational and cultural exchanges between students world-wide;
- cultural, vocational, social and leisure use in libraries, clubs and at home;
- access to experts in many fields for students and staff;
- staff professional development through access to national developments, educational materials and good curriculum practice;
- communication with support services, professional associations and colleagues;
- improved access to technical support including remote management of networks;
- share teaching materials with students and parents via Class Charts;
- use of AI technology and generative content to support the learning process; and
- signpost students and parents to relevant online safeguarding support agencies.

How will the Internet enhance learning?

- The school Internet access is designed expressly for student use and will include filtering for all staff and student accounts.
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Staff should guide students in on-line activities that will support the learning outcomes planned for the students' age and maturity.

- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation and the support accessible from AI technologies and generative content.

Students will learn to evaluate Internet content

- If staff or students discover unsuitable sites, the URL (web site address) and content must be reported to IT Support. This will then be forwarded to Link2ICT and the relevant website will be blocked.
- Staff should ensure that the use of Internet derived materials by themselves and by students complies with copyright law.
- Students will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy, including generative AI content.
- Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

New technologies
Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, Internet access, collaboration, multimedia tools and AI technologies. A risk assessment needs to be undertaken on each new technology for effective and safe practice in classroom.

New applications are continually being developed based on the Internet, the mobile phone network, wireless, Bluetooth or infrared connections. Users can be mobile using a phone, games console or personal digital assistant with wireless Internet access.

We use regular online safety training, through the National Online Safety Forum, to ensure all members of staff, keep up to date with new technologies, latest devices, platforms, apps and trends. This ensures staff are fully aware of the increasing risks that exist on-line so they can tailor their teaching and pastoral care to the specific needs of students.

Section 3 - Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the school:

Governors
All Governors are required to undertake safeguarding and child protection training, including online safety, at their induction and annually. Governors have overall strategic responsibility for filtering and monitoring systems in school and are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors /Sub Committee receiving regular information about online safety incidents and monitoring reports.

The Chair of the Governing Body has taken on the wider role of Safeguarding Governor and is responsible for ensuring filtering and monitoring systems, which now requires a consideration of any AI tools and technologies in use. Reviewing the effectiveness of the school's online safety, including the monitoring of online safety and Smoothwall violation logs and filtering provision, is an important aspect of this role. However, the Governing Body are mindful that 'over-blocking'

can lead to unreasonable restrictions on what children can be taught with regards to on-line teaching and safeguarding. This applies equally to different forms of remote learning.

Headteacher and Senior Leaders:
The Headteacher has a duty of care for ensuring the safety (including online safety and remote learning) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Designated Safeguarding Leader.

- The Headteacher and members of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Headteacher and Senior Leaders are responsible for ensuring that staff receive suitable training to enable them to carry out their roles online safely.
- The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal online safety monitoring role.
- At Hillcrest School there is a policy and procedure for Safeguarding Supervision, designed by the DSL and includes online safety. This is to provide a safety net and support to those colleagues who take on important monitoring roles.

Designated Safeguarding Leader:
- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents.
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides regular safeguarding / online safety training and updated advice for staff through the National Online Safety Forum, including annual cyber-security training and the use of AI technologies to support learning.
- liaises with school IT technical staff to ensure effective filtering and monitoring, and reporting systems in place.
- completes an annual review of filtering and monitoring systems, or when a safeguarding risk is identified, there is a change in working practice or new technology is introduced, ie – the development of AI technologies as a learning tool.
- creates communication channels for students and parents to report any online safety concerns, i.e. – cyber-bullying, harassment, child-on-child abuse, cybercrime, inappropriate content, including AI generated imagery and content.
- plans and co-ordinates curriculum provision, i.e. – Internet Safety Day, Life Skills provision, planning online safety assembly every half-term.
- takes appropriate disciplinary action against students for inappropriate behaviour online, as outlined in the Behaviour and Anti-Bullying policy.
- raise awareness with staff about the potential impact of remote learning on the mental health and well-being of students, including screen time, during periods of remote learning;.
- receives reports of online safety incidents/violations and creates a log of incidents, and actions taken, to identify patterns in student online behaviour and inform future online safety developments.
- meets regularly with Safeguarding Governor to discuss current issues, review incident logs and filtering / change control logs, and reports termly to the Governing Body.
- audits current provision for online safety education through the 360-degree tool.

- applies school safeguarding practices and makes appropriate referrals to external agencies if online behaviour suggests a child may be at risk of harm.
- signposts parents/carers to appropriate online safety resources to support them to keep their child safe online through the National Online Safety Forum.

ICT Operations Manager:
The ICT Operations Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack.
- that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed.
- the filtering policy, is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- that they keep up to date with online safety technical information, including the use of any AI technologies, to effectively carry out their online safety role and to inform and update others as relevant.
- that the use of the network / internet/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction.
- that monitoring software / systems are implemented and updated as agreed in school policies, including the monitoring of all school loaned technology used by staff and students out of school.

Teaching and Support Staff (including trainee teachers, volunteers and supply staff)
Are responsible for ensuring that:

- they have an up-to-date awareness of online safety matters and of the current school Online Safety Policy and practices.
- attend and complete all safeguarding training in school, including annual cyber-security training.
- report any possible safeguarding or welfare concerns to the DSL during any form of face-to-face or remote communication with students.
- they have read, understood and signed the Staff Acceptable Use Policy (AUP).
- they report any suspected misuse to the Headteacher and/or DSL (ie - when they witness of suspect unsuitable material has been accessed; there is failure in the software or abuse in the system; and they notice abbreviations or misspellings that allows access to restricted material).
- notify the ICT Manager and DSL when they are teaching topics which could create unusual activity on filtering logs or there are perceived unreasonable restrictions that affect teaching and learning activities.
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems, particularly during remote and live learning.
- online safety issues are embedded in all aspects of the curriculum and other activities.
- pupils understand and follow the Online Safety Policy and acceptable use policies.
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices.

- in lessons where internet use is pre-planned, pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches, particularly when using any form of AI tools or technologies.
- review resources, even when from a trusted source, to ensure all sites and resources used, both in lessons and remotely, are age and content appropriate.

Students:

- are responsible for using the school digital technology systems in accordance with the 'Acceptable Use Agreement'.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good online safety practice when using digital technologies out of school, including the use of school loaned technology, and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents/Carers:

- Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way.
- The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, ParentMail, website and information about national / local online safety campaigns / literature.
- Guidance is shared with parents/carers to emphasise the importance of working with their child to create a safe online environment, particularly regarding periods of remote learning, through setting age-appropriate parental controls on digital devices and using internet filters to block malicious or inappropriate websites.
- During periods of remote learning, parents/carers will be made aware of what their child is being asked to do online, including the sites they will be asked to access and whom from the school (if anyone) their child is going to be interacting with online
- Parents/Carers may choose to supplement the school remote learning programme with support from online companies and, in some cases, individual tutors. In our communication with parents/carers we will emphasize the importance of securing online support from a reputable organisation/individual who can provide evidence that they are safe and trusted to have access to children.
- Parents/Carers will be informed of the systems to report any online safeguarding concerns, particularly during any remote learning periods.
- Parents are signposted to practical support available for reporting harmful or upsetting content as well as bullying, harassment and online abuse.
- Parents and carers will be encouraged to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of digital and video images taken at school events, access to parents' sections of the website and links provided to parental online safety courses on the National Online Safety Forum.

Section 4: Information Systems Security

Local Area Network (LAN)

- Users must take responsibility for their network use.
- All users will be issued with a username and password. Users must ensure that they log off when leaving a computer unattended.
- Passwords must not be made available to any other user
- Servers must be located securely and physical access restricted.
- The server operating system must be current with all security updates installed.
- Virus protection for the whole network must be current.
- Access by wireless devices must be actively managed.

Wide Area Network

- Personal data sent over the internet or taken off site must be encrypted. Staff can be provided with encrypted school purchased memory sticks and all staff laptops will be encrypted. Under the Data Protection Act the school may be fined £500,000 and individual staff up to £10,000 if school data / information is accessed externally.
- Any non-school memory sticks used by staff must be encrypted if they wish to use the device on school machines. Data from non-school memory sticks should be transferred to new school provided encrypted memory sticks.
- The IT support team do not recommend the use of USB devices to store data. Date used off site should be stored in OneDrive.
- Unapproved software will not be allowed in students' work areas or be attached to an email
- Virus protection will be installed and updated regularly.
- Files on the school's network will be regularly checked. Any inappropriate material will be removed with further actions or sanctions taken as necessary.

Wireless Network

- All users have a requirement to maintain the security of the network and must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Appropriate staff mobile devices will be given access to the Hillcrest wireless network and have the connection details entered by the senior ICT technician. The password will remain confidential.
- When the students leave the school, the device will then be denied all access to the wireless network by MAC filtering.

Managing E-mail accounts and access

- E-mail should not be considered private, and the school reserves the right to monitor all e-mail accounts
- Students may only use approved e-mail accounts on the school system.
- Access in school to external personal e-mail accounts will be blocked
- Student email accounts are restricted to internal use only (expect Sixth form accounts)
- Staff must only use school e-mail accounts to communicate with students

- Students must immediately tell a teacher or IT Support if they receive offensive e-mail.
- Students must not reveal details of themselves or others in e-mail communication, such as address or telephone number, or arrange to meet anyone.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.
- The forwarding of inappropriate messages is not permitted

Internet Access

The school's internet is filtered by Surfprotect (member of the Internet Watch Foundation and signed up to the Counter-~Terrorism Internet Referral Unit). Additional filters are available through monitoring software that have been purchased to ensure that students are making appropriate use of the internet. Internet access is granted to all staff and students on the basis of educational need. The filtering system is key to our role in safeguarding children from all potential online risks associated with child sexual exploitation, forced marriage, recruitment in gangs, people trafficking and radicalisation by extremist groups. Such monitoring, where possible, will continue during periods of remote learning and when students have school-loaned devices at home. The filtering system is applied to all school users, including guest accounts, school owned devices and devices using the school's broadband connection. The system filters all internet feeds, including back-up connections; handles multilingual web contents, images, common misspellings and abbreviations; identifies technologies and techniques that allow users to get around the filtering system; and provides alerts when any web content has been blocked.

The DSL will monitor all Smoothwall violations and report any concerns to appropriate external services as required, ie – Children's Social Care, Police, Channel. The DSL will also share any concerns with social workers or Family support workers already engaged with families, as required.

Managing Web site content

- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or students' home information will not be published.
- Web site photographs that include students will be selected carefully and will not enable individual students to be clearly identified.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- The copyright of all material will be held by the school or be attributed to the owner where permission to reproduce has been obtained.

Managing Emerging Internet applications

- Emerging technologies and the use of AI tools will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

Internet access records

- By using the Internet, secondary students are agreeing to abide by the Responsible Internet Use statement.
- Students who require Internet access should sign the Wi-Fi form agreement.

- Parents will be asked to sign and return a form stating that they have read and understood the Acceptable Use Policy before the student is issued with their username and password by IT Support.

- Staff and students will be asked to sign the Acceptable Use Policy at the start of each academic year.

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications (office group access has now been removed)

The risks will be assessed

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.

Management of filtering

- The school will work in partnership with the LEA, DfES and the Internet Service Provider to ensure systems to protect students are reviewed and improved.
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the ICT Operation Manager.

Section 5: Guidance for students

Social networking sites provide free, easy to use facilities. The school will control access to social media and social networking sites over the school network, including when using school-loaned technology at home. Students will be encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

- Students will be advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs
- Students are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph which could identify the student or his/her location.
- Students are advised on security and required to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others by making profiles private.
- Students are advised to not allow other members of their family or friends use the school technology that has been loaned to them at home.
- Students are advised that school loaned technology is to be used at home to complete school work – it should not be used for any other purposes, ie – playing games or online shopping.

Dissemination of rules and guidance to students

- Rules for Internet access will be posted in all rooms where computers are used.
- Students will be informed that Internet use will be monitored.
- Students will be asked to sign the Acceptable Use at the start of each academic year
- Instruction/reminder in responsible and safe use will precede Internet access.
- The rules regarding safe and acceptable use of ICT facilities is an integral part of the ICT and Life Skills curriculum. There is an online safety assembly every half-term.

Consequences for failure to follow Acceptable Use Policy

Online safety is an integral part of the school's 'Getting It Right' system. The school does not take responsibility for inappropriate use of digital media outside of school hours or outside of the school premises. Such issues which affect the running of the school, including child-on-child abuse, cyberbullying, sexual harassment or violence, and hate crime, will result in the involvement of any appropriate agency (e.g. the Police, Early Help, Children's Social Care) and the school following the 'Getting it Right policy towards the individual. Under the GIR system the following consequences may be issued:

- Students using inappropriate websites in lessons will receive a C1
- Students downloading inappropriate material from the internet will receive a C2
- Students found sending inappropriate messages via the internet will receive a C3
- Recording conversations, making videos or taking photographs of any member of the school community, without their permission, is not allowed. The recording, displaying, supply or posting of any such materials will result in a **fixed term suspension** up to ten days or possible permanent exclusion based on the nature and seriousness of the content posted. The school reserves the right to determine the length of any fixed term suspensions.

As part of our wider safeguarding provision, systems are in place for students to report all forms of abuse they may experience, including online and out of school. The systems are well promoted and easily accessible to all students. Students are aware that this includes online

behaviour that takes the form of abusive or harassing messages, the non-consensual sharing of indecent images, especially around group chats, and the sharing of abusive images and pornography, to those who do not want to receive such content.

Safeguarding: Cyber-bullying

Cyber-bullying is defined as "The use of Information Communication Technology, particularly mobile phones and the internet to deliberately hurt or upset someone" DCSF 2007. It is essential that young people, school staff and parents and carers understand how cyber-bullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users supports innovation and safety. Cyber-bullying will not be tolerated in school and is outlined as an example of 'child-on-child abuse' in 'Keeping children Safe in Education' (September 2025). Further details are set out in the Anti-Bullying policy and Behaviour policy.

- All incidents of cyber bullying reported to the school will be recorded.
- All reported incidents or allegations of cyber bullying will be investigated.
- If the school has reasonable grounds to suspect a student has been the victim of cyber-bullying, the perpetrator(s) may receive a fixed term suspension. Depending on the nature of the content this may result in a permanent exclusion.
- Students, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school reserves the right to involve any external agency deemed appropriate to resolve child-on-child and cyber-bullying issues on and out of school, i.e. – police, Early Help, Children's social care.

Personal Mobile devices (phones, smart watches, tablets and other mobile devices)

- Mobile devices brought into school are entirely at the staff member, students and parents or visitor's own risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device brought into school.
- Student personal mobile devices, which are brought into school, must be turned off (not placed on silent) and stored out of sight on arrival at school. They must remain turned off and out of sight from the moment the student walks through the school gate at the start of the day until they leave through the school gates at the end of the day.
- If students bring a mobile phone or personally owned device into school and are seen using the device ***anytime*** during the school day (including before and after school school), the device will be confiscated, the student will receive a C3 consequence and a 60-minute SLT detention. Parents will be contacted via ClassCharts and will be required to plan to collect the device from school. If the student refuses to hand their mobile phone to a member of staff, a one-day fixed term suspension will be issued, and the student will be required to hand their mobile phone into main reception for five days after returning from the suspension. If the student fails to do this, a further fixed term suspension will be issued.
- The Bluetooth or similar function of a mobile device should be always switched off and not be used to send images or files to other mobile devices.
- No images or videos should be taken on mobile devices without the prior consent of the person or people concerned.
- The Headteacher reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or

undesirable material, including pornography, AI generated imagery, violence, bullying, criminal activity or exploitation, or radicalisation. The Headteacher also reserves the right to contact the police to request support if the student refuses to co-operate and there are reasonable grounds to suspect the student and/or other members of the school community are at risk of harm.

Safeguarding: Radicalisation

We strongly recognize the risk posed to our students of on-line radicalization, as extremist organizations seek to radicalise young people by social media and the internet.

To combat this online threat, we use the Smoothwall system to filter and monitor student online behaviour daily, with specific focus on the growing use of AI tools and access to AI generated content. Trigger words, phrases and content is updated and reviewed on a regular basis.

The Headteacher and DSL are notified of any inappropriate online behaviour, and appropriate steps are taken as required. This may involve speaking to the student, contacting parents, setting up a mentoring programme or making a direct referral to Early Help, Children's social care, police or Channel based on the seriousness of the incident. Our annual staff training ensures all staff are fully aware of the risks posed by the online activity of extremist and terrorist groups.

Online safety is a key aspect of the school curriculum and equips pupils to stay safe online, both in school and outside. Online safety is delivered predominantly in the ICT curriculum with specific focus on the range of social media sites that could pose a threat to students. For example;

- Extremist groups use Facebook to share content, such as news stories and YouTube videos, among their peer groups. This is very common amongst far-right extremist groups in the UK such as Combat 18, Young Patriots, Christian Patrol, Blood and Honour, National Action and Britain First.
- Twitter is a popular platform for pro-ISIL and EDL accounts. It is easy to establish an account, stay relatively anonymous and share material.
- YouTube is used to host videos, both with official ISIL output and videos created by users themselves. Multiple 'dummy' accounts will be set up so that when videos are taken down, they can be reposted quickly.
- ASK.FM is sometimes used by people considering traveling to Syria or Iraq and provides information on travel, living standards, recruitment fighting and broader ideology.
- Instagram is used by fighters and ISIL supporters to share the photosets frequently used by ISIL media organisations.
- Tumblr is an online blogging site and is used by ISIL fighters to promote longer, theological reasons why people should travel to Syria and Iraq. It is popular with female ISIL supporters, who have written blogs addressing the concerns girls have about traveling to the region, such as leaving their families and living standards in Syria.
- Private messaging apps, such as WhatsApp, Tik-tok, Kik, SureSpot, Whisper, Yik Yak, Omegle and Viber, are also commonly used to share messages on what to pack to travel and who to contact when they arrive.

Online safety is also delivered in other subjects, the Life Skills curriculum and in our whole school assembly programme. Our annual Life Skills audit identifies the extent of curriculum coverage for this and all other safeguarding themes.

Online Safety: Child Criminal/Sexual Exploitation and sharing of nude/semi-nude images

Sexting is images or videos generated by children under the age of 18, or of children under the age of 18 that are of a sexual nature or are indecent. These images are shared between young people and/or adults via a mobile phone, handheld device or website with people they may not even know.

It is important to be aware that people involved in sharing sexual videos and pictures may be committing a criminal offence. Specifically, crimes involving indecent photographs (including pseudo images) of a person under 18 years of age fall under Section 1 of the Protection of Children Act 1978 and Section 160 Criminal Justice Act 1988. Under this legislation it is a crime to:

- take an indecent photograph or allow an indecent photograph to be taken, even if the image is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI generated imagery.
- make an indecent photograph (this includes downloading or opening an image that has been sent via email).
- distribute or show such an image.
- possess with the intention of distributing images.
- Advertise and possess such images.

Steps to be taken in the event of a disclosure

If a student discloses about a potential sexting issue, the member of staff must consider if the student disclosing about themselves receiving an image, sending an image or sharing an image?

- Is it an image, video or message?
- What sort of image is it? Is it potentially illegal or is it inappropriate?
- Who sent it?
- Is it a school device or a personal device?
- Does the student need immediate support and or protection?
- Are there other students and or young people involved?
- Are there any adults involved?
- Do they know where the image has ended up?
- How widely has the image been shared and is the device in their possession?

Initial disclosure may be to a class teacher, non-teaching member of staff or peer. If this is the case:

- Safeguarding / Child Protection Policy must be followed
- Initial concern completed and reported immediately
- All disclosures must be passed on to the DSL / Safeguarding Team
- Clear record the incident should be made after referral to the DSL / Safeguarding Team
- The Headteacher should be informed
- There may be instances where the image needs to be viewed, and this should be done in accordance with protocols.
- Police should be informed of illegal activity

Searching a device

A device can be examined, confiscated and securely stored if there is reason to believe it contains indecent images or extreme pornography. The revised Education Act 2011 gives schools

the power to seize and search an electronic device if they think there is good reason for doing so. When searching a mobile device, the following conditions apply:

- The action is in accordance with the school's child protection and safeguarding policies
- The search is conducted by the head teacher or a person authorised by them
- A member of the safeguarding team is present
- The search is conducted by a member of the same sex

Never .....

- Search a mobile device even in response to an allegation or disclosure if this is likely to cause additional stress to the student/young person UNLESS there is clear evidence to suggest that there is an immediate problem
- Print out any material for evidence
- Move any material from one storage device to another

Always...

- Inform the school Designated Safeguarding Lead (DSL)
- Record the incident
- Act in accordance with school safeguarding and child protection policies and procedures
- Inform relevant Senior Leadership Team about the alleged incident before searching a device

If the image has been shared across a personal mobile device:

Always..

- Confiscate and secure the device(s)

Never...

- View the image unless there is a clear reason to do so
- Send, share or save the image anywhere
- Allow students to do any of the above

If the image has been shared across the school network, website or social network:

Always..

- Block the network to all users and isolate the image

Never...

- Send or print the image
- Move the material from one place to another
- View the image outside of the protocols in your safeguarding and child protection policies and procedures

If indecent images of a child are found the Safeguarding Team will;

- Store the device securely
- Carry out a risk assessment in relation to the young person
- Make a referral if needed to Early Help or Children's Social Care
- Contact the police (if appropriate) it is not the responsibility of a school to make decisions about the seriousness of the matter

- Put the necessary safeguards in place for the student, e.g. they may need counselling support, immediate protection and parents must also be informed.
- Inform parents and/or carers about the incident, how it is being managed and provide guidance/support on removing the image from the internet.

The safeguarding Team will always make a Child Protection referral to the police and Children's Social Care if:

- the incident involves an adult
- there is reason to believe that the child has been coerced, blackmailed or groomed, or there are concerns about their capacity to consent
- the content depicts sexual acts which are unusual for the child's developmental stage or are violent.

We are aware that there may be a multitude of reasons why a student has engaged in sexting – it may be a romantic/sexual exploration scenario, or it may be due to coercion. It is important to remember that it won't always be appropriate to inform the police; this will depend on the nature of the incident. However, as a school it is important that we record incidents are consistently. It may also be necessary to assist the young person in removing the image from a website or elsewhere.

While any decision to charge individuals for such offences is a matter for the Crown Prosecution Service, it is unlikely to be considered in the public's interest to prosecute children. However, children need to be aware that they may be breaking the law. Although unlikely to be prosecuted, children and young people who send or possess images may be visited by police and on some occasion's media equipment could be removed. This is more likely if they have distributed images. However, there are cases in which children and young people have been convicted and sent to prison. The important thing to remember is that whilst, as a school, we need to consider the implications of passing an incident over to the police, it is not the responsibility of the school to make decisions about the seriousness of the matter. Clearly, if it is a case that involves an adult, the process and potential outcome will be very different.

Containment and Student Reaction

There are cases in which victims have had to leave or change schools because of the impact of the incident. As a school we will endeavour to provide necessary support for students.

- Anxiety - who has seen the image and where it has ended up.
- Reassurance - regarding its removal from the platform on which it was shared.
- Support - from the school, their parents and their friends.
- Observation - parents should usually be told what has happened so that they can keep a watchful eye over their child
- Curriculum - reinforce to all students the impact and severe consequences that this behaviour can have.

Safeguarding - Sexual harassment and violence

In 'Keeping Children Safe in Education' (September 2025), sexual harassment is defined as 'unwanted conduct of a sexual nature that can occur online and offline and both inside and outside of school'. This includes:

- Sexual comments, i.e. – telling sexual stories, making lewd comments, making sexual remarks about clothes and appearance, taunts, innuendoes, propositions, sexual jokes, calling someone sexualised names.
- Distributing sexual material (including pornography) and sending photos or videos of a sexual nature, even if they use AI generated imagery.
- Displaying pictures, photographs or drawings of a sexual nature.
- Online harassment, i.e. – consensual or non-consensual sharing of nude and semi-nude images and videos, sharing unwanted explicit content, coercion, threats, sexual exploitation and grooming.
- Making phone calls and sending texts or messages of a sexual nature.
- 'Games' with a sexual element that may make a child or young person feel uncomfortable or scared (e.g. taking clothes off, kissing or touching games).
- Pressure to be in a relationship with another person, or to engage in a sexual act with another person – both inside and outside of school.
- Sexism in all its forms; pressure to conform to gender 'norms' (e.g. pressure on children to have multiple partners, or pressure on boys and girls to be heterosexual).

All forms of sexual harassment, online sexual abuse and sexual violence (including sexualised language) is unacceptable, and we have a zero-tolerance approach. Abusive comments and interactions, including online, should never be passed off or dismissed as 'banter' or 'part of growing up'. Nor will harmful sexual behaviour be dismissed as the same or 'just having a laugh'. All reports child-on-child abuse will be treated as a safeguarding matter and in line with our Child Protection and Behaviour policies.

Section 6 – Curriculum, Teaching and Learning

As outlined in 'Teaching on-line safety in schools' (DFE – June 2019), our whole school curriculum is designed to teach students about the underpinning knowledge and behaviours that can help them to thrive and navigate the on-line world safely and confidently, as well as the many risks that exist on-line. This is particularly important in relation to new DFE guidance on 'Relationships Education, 'Relationships and Sex Education' and 'Health Education' (September 2025), as each focus significantly on ensuring students understand how to stay safe and behave positively, responsibly, respectfully and securely on-line. Teachers will address online safety and behaviour in a sensitive and age-appropriate manner.

In accordance with 'Education for a connected world' – UK Council for Internet Safety (November 2020), the curriculum content, including Life Skills lessons, half-termly assembly themes, form programme activities, workshops delivered by external visitors and peer mentoring, will support students to ensure they confidently know how to:

- **Evaluate what they see online** (i.e. – cookies; fake URL or websites or email addresses; hoaxes; harmful online challenges, scam emails; fraud; is the content fact or opinion; misinformation, disinformation, fake news and conspiracy theories; is the person who they say there are and why do they want certain personal information; phishing)

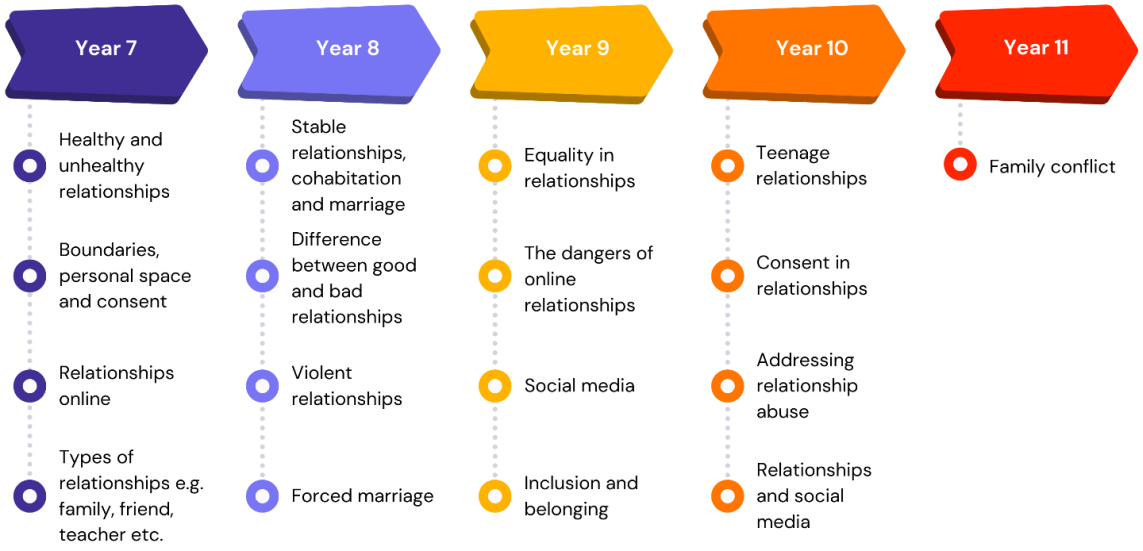
- **Recognise techniques used for persuasion** (i.e. – on-line content which misleads people or encourages them to believe something that is false; techniques used by companies to persuade people to buy something; ways in which games and social media companies try to keep users on-line longer; inappropriate advertising)

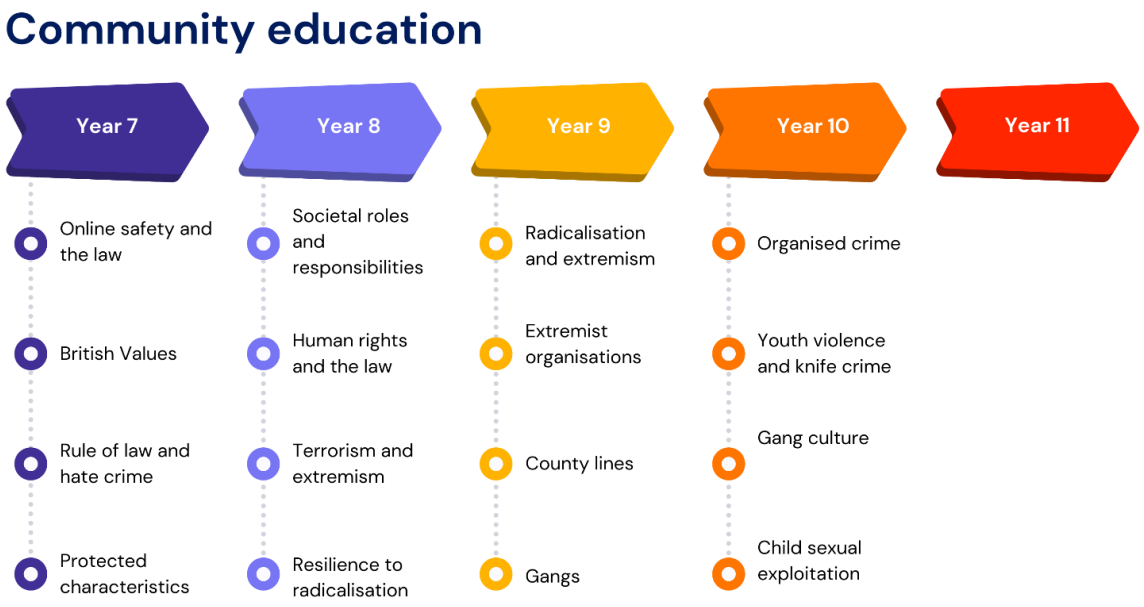
- **On-line behaviour** (i.e. – self-image and identity; online relationships; help students to identify what is acceptable and unacceptable behaviour on-line (including what constitutes child-on-child abuse, sexual harassment, criminal and sexual exploitation); understand why people behave differently online; understand how online emotions can be intensified resulting in a mob mentality approach; techniques to defuse online arguments and negative language increasingly used in online games)

- **Identify on-line risks** (i.e. – how can students put themselves at risk on-line; privacy settings; importance and relevance of age restrictions; when taking a risk can be positive and negative; on-line reputation and impact on digital footprints; risks and benefits of sharing information on-line; copyright and ownership; cyber-dependent crime; online gambling; risks with live streaming sites and how to make a judgement about when and how to share)

- **Seek and access support** – this will enable students to understand safe ways in which to seek support if they are concerned or upset by activity on-line, including how to report online concerns, remove inappropriate content and the potential risks using AI chatbots. We recognise the negative impact this can have on a person's confidence, self-esteem, physical health and mental health. Therefore, signposting to appropriate sources of support is vitally important, as well as students knowing how to access this support.

Relationships education





Teachers recognise that it is crucial to create a safe environment in which students feel comfortable to talk about something which happened to them on-line. This is particularly important for vulnerable students, particularly those Looked After and/or with Special Educational Needs, who may be more susceptible to on-line harm and may have greater reliance on AI tools and content for support purposes. The DSL will share relevant information with staff, particularly when teaching on-line safety to students who have previously been abused or harmed on-line. Children with SEND may require different teaching methods to learn about online safety, such as:

- Tailored teaching materials, including visual, verbal and multi-media resources
- More detailed explanation of complex issues
- Continuous reminders and reinforcement of online safety messages
- A slower, smaller step approach to building online resilience

As outlined in 'Teaching online safety in schools' (June 2019), teaching staff will consider the appropriateness of online resources, even when they are from a trusted source, to ensure they are appropriate for the cohort of students. Staff will consider:

- Where does the organisation/website get their information from?
- What is their evidence base?
- Have they been externally quality assured?

The same consideration will also be given to online resources and materials used by any external visitors coming into school. Staff will use the 'Guidance for educational settings seeking support from external agencies', developed by the UK Council for Internet Safety, to guide their process of selecting suitable visitors and sessions.

Section 7: Guidance for Staff (including trainee teachers, volunteers and supply staff)

Remote Learning (including Live Learning)
As outlined in the updated guidance from the Safer Recruitment Consortium (February 2022), staff should only contact students through school approved platforms or school email accounts.

This ensures appropriate filtering and monitoring software is enabled during periods of remote learning, as well as ensuring online tools are in line with privacy and GDPR requirements.

As part of any remote learning provision, the senior leadership team and curriculum managers will consider whether there are alternatives to live learning lessons, i.e. – using audio only, pre-recorded lessons, existing online resources

Virtual live lessons should be timetabled and occur within operating times agreed by the Headteacher. A senior member of staff, DSL and/or Curriculum Learning Manager will be able to drop into any virtual lesson at any time. Registers of any live lessons should be taken, including those who arrived late or left early and clear notes should be made of any problems or issues that occurred and how these were resolved. One to one tutoring is not encouraged but if it does happen it should be authorised by the Headteacher, and a parent or another member of staff must also participate in the one-to-one meeting.

Staff engaging in remote learning, whether live or pre-recorded, should display the same standards of dress and conduct that they would do in the real world. In addition, students should be appropriately dressed if the lesson is delivered live. They should ensure that they use a neutral area where nothing personal or inappropriate can be seen or heard in the background. Staff and students should be in living/communal areas in their homes – not their bedrooms.

Any resources or videos used, either during live or pre-recorded learning, must be age appropriate as the student may not have support immediately on hand at home if they feel distressed about the content.

Teachers should not contact students outside the operating times defined by the Headteacher, take or record images of students for their personal use or record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by the Headteacher). If a teacher wishes to record a lesson, they should secure permission from the Headteacher and gain parent/student consent in regard to the retention and storage of the recording. If a teacher is concerned that a student or parent is recording the lesson or one-to-one meeting, without their prior knowledge or consent, they should either end the lesson immediately or block the student/parent from the lesson.

Social Media

All staff are made aware of the potential risks of using social networking sites or personal publishing either professionally with students or personally. They are made aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status. Staff should not refer to Hillcrest school, other educational institutions, work related activities or make comments on national education policy on such sites that may bring the school or teaching profession into disrepute. Staff are discouraged from expressing political, religious, cultural or socio-economic views on any forms of social media as comments could be perceived as undermining the teaching profession. Staff should be aware that they are always representing the school and profession in the community and that other members of the community may know the school the member of staff works at even though it is not listed on their personal profile or referred to in comments made on different social media sites.

Privacy settings should be high and updated regularly, i.e. – Facebook accounts must be set at 'friends' level only. Staff must not post any images of other members of staff on such sites without their permission. Staff must not, under any circumstances, post images of students on

such sites. In addition, staff are discouraged from posting images of their children, family or themselves involved in social activities that may undermine their role as a teacher, i.e. – posting images of themselves inebriated out of school. Staff are encouraged to remove personal images as profile pictures and ensure that their employment details, personal telephone numbers or email address are not recorded on personal details sections of any social media site.

Staff must not engage in social network activity with current and previous students or parents under all circumstances.

E-Mail Accounts

Staff are given a school e-mail address which should be used for professional communication only. Staff should not give their personal e-mail address to students or parents under any circumstances. Staff should only contact students via their school e-mail account. Staff should not reply to an e-mail from a student if it is sent from the student's personal e-mail account. Staff should be aware that e-mail activity is monitored by IT Network Support.

Internet access and websites

Any material accessed by staff that the school believes is illegal will be reported to appropriate agencies such as the Police. Accessing material considered inappropriate may result in the school initiating disciplinary actions against staff members as necessary. The school will regularly monitor staff internet activity on school lap equipment in and out of school. This monitoring will be carried out by a member of the Senior Leadership Team.

Use of school equipment

Staff are issued with laptops on arrival at the school. The laptop is school property and should be explicitly used for appropriate school related business. The school, however, recognises that occasional and appropriate personal use of the school's computers is beneficial both to the development of IT skills and for maintaining a positive work-life balance.

During working hours staff must use school equipment for work-related activities only. It is prohibited to use school equipment at any time for inappropriate personal use. Among uses that are considered inappropriate are the following:

- Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
- Making ethnic, sexual preference, or gender related slurs or jokes

Staff should be aware that any work uploaded to a laptop is automatically synced to the school servers.

Use of student images

Images of a student must not be published without the parent's or carer's written permission. This permission is obtained when a student first joins the school. Staff should not use their own personal devices to take and store images of students. School cameras should always be used. All images of students should be stored on the school network and not on individual staff memory sticks. Staff should store all school-based photographs on the 'Photo Drive' on the shared staff area. All photographs will be deleted at the end of each academic year.

Data Protection
Staff must be made aware of their responsibility to maintain confidentiality of school information. Staff are personally responsible and liable if they lose any school data, i.e. – theft of laptop or memory stick containing school data. Under the Data Protection Act the school may be fined £500,000 and individual staff up to £10,000 if school data / information is accessed externally.

Mobile Phones / devices
All mobile phones brought on site should be PIN protected in case of theft or loss. Staff must not use any form of personal devices to take and store photographs of students.

The recording, taking and sharing of images, video and audio on any personal mobile device is to be avoided, except where it has been explicitly agreed by the Headteacher. Such authorised use is to be recorded. All mobile device use is to be open to monitoring scrutiny and the Headteacher is able to withdraw or restrict authorisation for use at any time if it is deemed necessary.

The Headteacher reserves the right to search the content of any mobile devices on the school premises where there is a reasonable suspicion that it may contain illegal or undesirable material, including pornography, harassment, violence or bullying. Staff mobiles devices may be searched at any time as part of routine monitoring.

Student use of staff laptops
Staff should not allow students to use their school laptop as students may gain access to confidential information or use the internet for inappropriate purposes. Staff should not leave their lap top unattended. It is essential that staff lock their computer if students are left unsupervised for a period of time.

Staff Files
Staff should be aware that IT Network Support staff can access the content of all staff folders as necessary without permission from the individual member of staff.

Dissemination of rules for staff
- All staff are governed by the terms of the 'Responsible Internet Use' in school.
- All staff including teachers, supply staff, teaching assistants and support staff, will be provided with the School Online Safety Policy, and its importance explained.
- Staff should be aware that Internet traffic is filtered and traced to the individual user. Discretion and professional conduct is essential.
- The monitoring of Internet use is a sensitive matter and will be conducted by a member of the Senior Leadership Team.
- Staff development in safe and responsible Internet use and on the school Internet policy will be provided annually.

Complaints Procedure Regarding Internet Use
- Responsibility for handling incidents will be delegated to a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Students and parents will be informed of the complaint's procedure.

Section 8: Parental Support (see appendix 1)

- Parents' attention will be drawn to the On-line Safety policy in newsletters, the school prospectus and on the school Web site, as well as through literature issued and practical demonstrations given at Parents Evenings and other school events.
- Information will be shared with parents/courses about courses they can access and complete through the 'National Online Safety Forum' to develop their understanding of how to best keep their child(ren) safe online.
- The school will update the annual parent guide on online safety and upload to the website. This is particularly relevant to the threat of online radicalisation by extremist ideologies. Information is provided for parents / carers on possible signs to suggest their child is at risk of becoming radicalised and parents / carers are signposted on the website to support organisations including THINKUKNOW, CHANNEL, FAST, INTERNET MATTERS, CHILDNETLONDON GRID FOR LEARNING, NETAWARE and UK SAFER INTERNET CENTRE. The website also contains general information for parents / carers on how to keep their child safe from other online dangers included sexual harassment, child sexual exploitation, involvement in gangs and people trafficking.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- A partnership approach with parents will be encouraged. This could include demonstrations, practical sessions and suggestions for safe Internet use at home.

Section 9: Internet Use within the school community

- Students and all adult users will need to sign the acceptable use policy.
- Parents/carers of children under 16 years of age will be required to sign an acceptable use policy on behalf of the child.
- Visitors must agree to the code of conduct which is displayed during the user's logon to the network.

Section 10: Monitoring

Our Internet and Online Safety Policy has been written by the school. It has been agreed by the senior management and approved by governors. It will be reviewed annually.

Name of responsible person: Steven Connor-Hemming

Date reviewed: September 2025

Date of next review: September 2026