

WHITGIFT SCHOOL

ONLINE SAFETY POLICY

Staff responsible for this policy:

Oz Bhatti (Deputy Head (Pastoral))

Email: oab@whitgift.co.uk

Ally Tiltman-Phillips (Director of Safeguarding/Designated Safeguarding Lead, (DSL))

Email: a.tiltman-phillips@whitgift.co.uk

Policy reviewed: August 2026

Next review: August 2027

1. Policy statement

Whitgift School recognises the vast opportunities that the internet and digital technologies offer to both staff and students. Whitgift's approach to online safety is underpinned by the School's values of Belonging, Respect, Courage, Curiosity and Ambition. These values guide students in developing positive digital behaviours, exercising good judgement online, engaging respectfully with others and navigating digital environments safely, responsibly and ethically. The School also acknowledges the associated risks, including but not limited to instances of sexual grooming via chatrooms, bullying, stalking, radicalisation, sextortion, AI deepfakes, nudification apps, synthetic imagery, misinformation, disinformation and online fraud. We are committed to raising awareness of the potential risks ensuring that our students are equipped with the knowledge, skills, and support necessary to navigate the online world safely and responsibly.

Whitgift School understands its responsibilities include:

- **Education and Awareness:** Providing students with age-appropriate education on online safety, including critical thinking skills and responsible digital behaviour, to enable them to remain safe and within the law when using the internet and related technologies in and beyond the classroom.

- **Student Voice and Engagement:** Creating opportunities for students to discuss online safety concerns, share their experiences, and contribute ideas to improve our digital safeguarding practices.
- **Safe Online Environment:** Maintaining a secure and monitored online environment within the School's digital infrastructure to protect students from potential harm.
- **Intervention and Support:** Implementing effective mechanisms to identify, respond to, and escalate online safety concerns promptly and appropriately.
- **Digital Citizenship:** Promoting respectful, responsible and ethical participation in digital communities and online spaces.

This policy is designed to safeguard the welfare of all students, provide a framework for the safe and responsible use of IT systems, and to clearly define individual responsibilities. It aims to:

- Provide clear guidance on how to minimise risks associated with online activity.
- Outline what is deemed in our context as acceptable behaviour and digital conduct.
- Establish clear structures by which online misdemeanours will be treated.
- Define the procedures for responding to online safety, particularly where there are doubts or concerns.

Online safety is a continuous and interconnected theme across many of Whitgift School's policies. This document should be read in conjunction with other school policies, including but not limited to:

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy
- Values, Recognition and Conduct Policy
- Boarding House Acceptable Use Policy
- Mobile Devices Acceptable Use Policy
- Searching a Student Policy
- Sexting Policy
- Social Media and Communications Policy
- Student Acceptable Use Policy
- Staff Code of Conduct
- Staff and Visitor Acceptable Use Policy
- Image Use Policy (*once published*)
- AI Policy

In the development of this policy, due regard was given to the following guidance:

- [DfE Filtering and Monitoring Standards](#)
- UKCIS [Sharing Nudes and Semi-Nudes](#): Advice for Education Settings Working with Children and Young People (2024)
- DfE [Keeping Children Safe in Education](#)(2026)
- DfE [Mobile Phones in Schools](#)(2026)
- DfE Teaching Online Safety in Schools (2023)

- DfE Relationships Education, Relationships and Sex Education (RSE) and Health Education (2025)
- Prevent Duty Guidance: England and Wales (2024)
- [DfE Generative Artificial Intelligence \(AI\) in Education Guidance](#)
- [Meeting Digital and Technology Standards in Schools and Colleges](#) (2026)
- UKCIS [Education for a Connected World](#) Framework (2020)
- UKCIS [Online Safety in Schools and Colleges: Questions from the Governing Board](#) (2022)
- UKCIS [Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People](#)
- UKCIS [Using External Expertise to Enhance Online Safety Education](#) (2022)
- UKSIC [Appropriate Filtering for Education Settings](#) (2024)
- UKSIC [Appropriate Monitoring for Schools](#) (2024)
-

The School recognises that, due to the quickly evolving nature of the online environment, terminology and technology is likely to change frequently and present new emerging risks. This policy is therefore subject to a thorough annual review. In addition to scheduled reviews, the policy will be updated as necessary in response to any new technological developments, emerging threats to online safety, or specific incidents or concerns arising within the School or the wider educational context.

2. Policy scope

This policy applies to all members of the School community, including students, staff¹, parents/carers, visitors and volunteers. It is not limited to activity on the School network; rather, it encompasses all aspects of online safety that may impact the School community including the welfare and reputation of individuals, as well as the culture and reputation of the School.

3. Roles and responsibilities

Online safety is a shared responsibility. To ensure the safeguarding of all members of the school community, it is important the whole community works together to:

- Model and develop safe and responsible online behaviours.
- Promote awareness, understanding and learning from each other of online risk.
- Reporting inappropriate online behaviours, concerns, or misuse as soon as they become apparent.
- Support one another in developing digital resilience.

3.1 Governors

The Governing Body holds overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. In relation to online safety, key responsibilities of the Governing Body include:

¹ References to staff includes all those who work for or on behalf of the School, regardless of their employment status, including supply staff, contractors, volunteers and Governors.

- Governors will receive at least annual assurance regarding the effectiveness of filtering and monitoring systems, online safety incidents, emerging online risks, and actions taken in response to identified concerns.
- Reviewing the effectiveness of this policy at least annually including the School's filtering and monitoring systems;
- Ensuring that all staff receive appropriate safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:
 - All staff are adequately trained about online safety;
 - All staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
 - Staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the School.
- Ensuring that Students are taught about safeguarding, including online safety, as part of providing a broad and balanced curriculum.
- Ensuring that online safety forms part of the School's wider safeguarding and child protection arrangements and that appropriate oversight exists for emerging technologies and online risks.

3.2 Headmaster and the Senior Leadership Team (SLT)

The Headmaster has a duty of care to ensure the safety (including online safety) of all members of the school community and fostering a culture of safeguarding. Together with the Senior Leadership Team (SLT), responsibilities include:

- Ensuring that emerging online risks, including risks arising from generative AI, deepfake technology and online exploitation, are considered as part of the School's wider safeguarding and risk management framework.
- Procuring appropriate filtering and monitoring systems.
- Documenting decisions related to online safety infrastructure, reviewing the effectiveness of the filtering and monitoring provisions.
- Overseeing reports and incidents related to online safety, ensuring appropriate follow-up.
- Ensuring staff are appropriately trained in fulfilling their online safety responsibilities.

3.3 Director of Safeguarding/Designated Safeguarding Lead (DSL)

The responsibilities of the Director of Safeguarding/DSL include:

- Taking the lead responsibility for safeguarding and child protection at the School; this includes the responsibility for online safety and understanding of the School's filtering and monitoring systems and processes.
- Ensuring that this policy is upheld at all times, working with the senior leadership team, and IT staff to achieve this. As such, in line with the School's Safeguarding and Child Protection Policy, the DSL will take appropriate action if in receipt of an incident report relating to an activity that has taken place online.

- Working closely with the School's IT staff to ensure that the requirements for filtering and monitoring are met and enforced as well as ensures that checks are properly made of the system.
- Meeting termly with the School's Safeguarding Governor to review and report on safeguarding and child protection matters, including online safety.

3.4 Head of Ideatum

The responsibilities of the Head of Ideatum include:

- Planning the Ideatum curriculum, identifying opportunity to teach digital literacy and online safety.
- Ensuring digital literacy and online safety is addressed repeatedly through a spiralling curriculum.
- Using real-life issues that young people may encounter whilst navigating online spaces, opportunities and challenges.
- Addressing online safety through content, contact, conduct and commerce
- Reviewing the impact of the Ideatum curriculum and adapt to meet the demands of the ever-changing online world and the risks it presents.
- Ensuring students develop critical thinking, media literacy and digital literacy skills that enable them to evaluate online content, identify misinformation and make informed decisions.

3.5 IT staff

The School's IT staff have a key role in maintaining a safe and secure network and technical infrastructure and staying informed with the rapid succession of technical developments. Their responsibilities include:

- Ensuring the security and integrity of the School's hardware and network systems.
- Collaborating with the Director of Safeguarding/DSL and SLT helping them make key strategic decisions related to safeguarding and technology.
- Technical responsibility for maintaining the School's filtering and monitoring systems, providing reports, and completing actions following concerns or system checks.

3.6 Staff

It is the responsibility of all staff to adhere to this policy, the School's Safeguarding and Child Protection Policy and other associated policies. The three principles of *Prevention*, *Protection* and *Support* should determine any action taken by a member of staff.

In addition, staff:

- Must be aware that technology can play a significant part in many safeguarding and wellbeing issues and that students are at risk of abuse online as well as face-to-face. Staff must also be aware that, sometimes, such abuse will take place concurrently online and during a student's daily life.
- Are expected to be alert to the possibility of students abusing their peers online and to understand that this can occur both inside and outside of school.

- Are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in and outside classrooms and to model positive attitudes and approaches to online safety.

As with all aspects of safeguarding and our strong focus on pastoral care, all staff members are responsible for promoting awareness and compliance with this policy. If members of staff wish to seek guidance on any aspect of online safety, they should consult the Director of Safeguarding/DSL.

3.7 Students

Students are expected to take an active role in maintaining a safe and respectful online environment. Key responsibilities include but are not limited to:

- Using the internet and technology in accordance with the Student Acceptable Use Policy, the Boarding House Acceptable Use Policy (as applicable).
- Knowing what action to take if they or someone they know feels worried or vulnerable when using online technology, at school, home or anywhere else.
- Recognising that information, images and content shared online may have long-term consequences and contribute to a permanent digital footprint.
- Recognising that information, images and content shared online may have long-term consequences and contribute to a permanent digital footprint.
- Reporting concerns about AI-generated, manipulated or synthetic content where it may cause harm, distress or place another person at risk.
- Understanding the importance of reporting abuse, misuse or access to inappropriate materials including any concerns about a member of staff or supply teacher. If any student suspects that a breach of this policy has been made by a member of the School community, it is their responsibility to report it as soon as possible to their Tutor or Head of Year, or in the case of a breach in the boarding house, to the Housemaster of Founder's House. They may also report a suspected breach to the Director of Safeguarding/DSL or any other member of staff.

3.8 Parents/carers

The role of parents in ensuring that their child understands how to stay safe online as well promoting safe and responsible practice in their own use of technology is crucial. Parents are encouraged to maintain an active interest in their child's online life, promote safe and responsible online behaviour, and engage with guidance provided by the School.

The School will contact parents if it has any concerns about students' online behaviour and likewise hopes that parents will feel able to share any concerns with the School.

Should parents have concerns that their son has been subjected to attempts of sexual grooming, radicalisation, sextortion/extortion, or other inappropriate online contact, or that they have received illegal content, they should contact the Designated Safeguarding Lead (DSL), the Head of Year, the Director of Section. as a matter of high importance. Where appropriate, the Director of Safeguarding/DSL will liaise with outside agencies, such as the Multi Agency Safeguarding Hub (MASH), the police and in particular CEOP (Child Exploitation and Online Protection) service.

Should parents wish to discuss any other aspect of online behaviour, such as possible online gaming addiction, or concerns about the amount of time spent online, they should similarly contact any of the relevant staff.

4. Education and awareness

The School considers itself to have a central role in educating students, parents and staff in online safety issues that may affect them. The School also recognises the relationship between online experiences, digital wellbeing and mental health, and seeks to help students develop healthy, balanced and sustainable relationships with technology. Whitgift recognises that technology can have both positive and negative effects on wellbeing. Online safety education therefore includes consideration of healthy technology use, balance, sleep, social connection, attention, self-image and emotional wellbeing in digital environments.

The breadth of issues classified within online safety can be categorised into four areas of risk, which staff, parents/carers and students should be aware of:

- **Content:** being exposed to illegal, inappropriate, or harmful material (e.g. pornography and violent sexual content, fake news, racist or extremist views, suicide, promoting self-harm or suicide)
- **Contact:** being subjected to harmful online interaction with other users (e.g. online grooming incl. sexual exploitation, radicalisation, personal data exploitation)
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm (e.g. making, sending, and receiving explicit images, or online bullying)
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams/fraud.

4.1 Online safety education for students

The safeguarding of all members of the community should be led by awareness of the issues and a sense of responsibility about how to behave in any given situation. Whilst regulation and technical solutions are particularly important, their use must be balanced by educating students to take a reasonable approach.

The School provides an age-appropriate, carefully sequenced programme that raises awareness of technical and behavioural aspects of online safety for students. This is predominantly delivered through Ideatum, a tailored programme, which contributes to the development of well-rounded critical thinkers. Further information about Ideatum can be found on the school website [here](#).

Assemblies, form time discussion activities, the marking of awareness days (e.g. Safer Internet Day), the use of technology in lessons and mechanisms, such as our Student Acceptable Use Policy, complement this provision. Where appropriate, the School also uses external speakers (e.g. Childnet) to enhance the School's online safety education. As appropriate, the School will follow the UKCIS guidance [Using External Expertise to Enhance Online Safety Education](#) (2022).

The Ideatum programme is designed to deliver information and explore issues at a level appropriate to the age, ability and emotional, physical and cognitive development of the student; certain topics will be revisited at appropriate points later in their development. Additionally, some content pertaining to online safety is covered in Digital Literacy lessons in the Lower First and First Form. Staff are encouraged to identify opportunities to thread online safety through school activities, both outside the classroom and within the curriculum.

The School's online safety programme addresses a wide range of online safety topics, including:

- Healthy digital behaviours and digital citizenship, including rights and personal protections;
- Digital consent and respectful online interactions;
- Balancing screen time;
- Passive and active online consumption;
- Digital behaviour disinhibition;
- Grooming, radicalisation and online abuse (including cybercrime, child criminal exploitation (CCE), cyberbullying, sextortion and acts of revenge pornography);
- Exposure to material that is not appropriate to their age, including pornography and that which may be self-made;
- Sharing of personal information;
- Privacy, personal data and online identity management;
- Hidden dangerous content;
- Online mis-dis-mal-information;
- Generative AI, deepfakes and synthetic content;
- Nudification applications and manipulated imagery;
- Online misogyny, harmful gender stereotypes and harmful online influencers;
- Online sexual harassment, coercive control and image-based abuse;
- Understanding the strengths, weaknesses and limitations of AI-generated content;
- Financial exploitation including cryptocurrency scams;
- Algorithmic influence and persuasive design features used by social media platforms.
- The use and impact of social media, including the social media algorithm;
- Digital addictions, including gaming, shopping and gambling; and
- Online reputations and digital footprints.

Before using external resources, the School will review the content of external teaching materials to ensure it is appropriate.

The School believes firmly in the principle of 'student voice' to address concerns and seek guidance on matters of online safety that directly affect the children and young people in our care. It encourages all members of the student body to feed back on issues addressed in Ideatum lessons, year group committee meetings, parents' evenings, and informally.

Student feedback regarding emerging platforms, applications and online trends will be considered as part of the School's ongoing assessment of online safety risks.

The School also recognises that effective online safety education needs to be tailored to the specific needs and vulnerabilities of individual students, including those who are victims of abuse, and those with special educational needs and disabilities. These considerations are embedded when devising and implementing processes and procedures to ensure the online safety of its students.

4.2 Online safety awareness and training for staff

New staff receive online safety training, as part of their safeguarding induction, which includes information on the school's expectations, applicable roles and responsibilities regarding filtering and monitoring.

During the mandatory safeguarding training, which takes place at least annually, staff are reminded of their individual responsibilities relating to safeguarding of children within the context of online safety and receive updates on current online safety topics. Where relevant, these are also addressed in the weekly Pastoral Bulletin email which is sent to all staff.

4.3 Online safety awareness and training for parents

Communication between home and school is vital in establishing good online safety principles and practice and therefore, the School seeks to work closely with parents in promoting a wide understanding of the benefits and risks related to internet and technology use.

There may be a gap between some parents' awareness of online safety issues, and the technical proficiency of their children. The School provides information and guidance to help bridge this gap through a variety of means, including parent workshops, newsletters, the school website and parents' evenings.

Should parents have any concerns over, or wish to seek guidance on, any aspect of online safety, they are encouraged to contact their son's tutor, Head of Year, the Head of Ideatum, the Director of Safeguarding/DSL or the Deputy Head (Pastoral).

5. IT infrastructure management

The School understands its responsibility for ensuring that the School's IT infrastructure is as safe and secure as is reasonably possible and aims to provide a safe environment to learn and work, including when online.

The School provides internet access and an email system as well as other technology to students and staff. Students and staff must adhere to the relevant Acceptable Use Policy when using technology on or off site. The use of the School's technology is monitored.

5.1 Technical security and data protection

The School's technical systems will be managed in ways that ensure that the School meets the recommended technical security requirements as outlined in DfE Meeting Digital Standards in Schools/Colleges (e.g. properly configured boundary firewall, up to date anti-malware software, clearly defined access rights for users).

The management of personal data is in line with data protection legislation and as outlined in the Data Protection Policy.

5.2 Filtering and monitoring

The School recognises that filtering and monitoring systems are important safeguarding tools but do not replace effective supervision, staff vigilance, education and professional judgement. It is therefore vital for staff to be aware of the systems in place and to play their part in feeding back about areas of concern, potential for students to bypass systems and any potential over blocking.

The Director of Safeguarding/DSL has lead responsibility for filtering and monitoring and works closely with the Director of IT to satisfy the [DfE Filtering and Monitoring Standards](#).

System checks are conducted when significant changes take place (e.g. technology, policy or legislation), in response to incidents and at least annually. Filtering and monitoring arrangements are reviewed annually and whenever significant changes occur to technology, safeguarding risks, legislation or pupil needs.

Staff, students and visitors should be aware that the School's filtering and monitoring systems apply to all users, all school owned devices and any devices connected to the School's internet. Deliberate access, or an attempt to access prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Values, Recognition and Conduct Policy.

5.2.1 Appropriate filtering

The School is responsible for ensuring that the School network is as safe and secure as possible, and undertakes to filter content without unreasonably impacting teaching and learning and restricting students from learning how to assess and manage risk themselves.

The School manages access to content using a filtering system that meets the standard defined in UKSIC Appropriate Filtering for Education Settings. As far as reasonably possible, access is denied to material that might prove to be of offensive, illegal, inappropriate or harmful nature. The effectiveness of the filtering system is regularly reviewed, but it has to be recognised that no filtering system can be 100% effective.

Where safeguarding concerns arise, these are highlighted to the Director of Safeguarding/Designated Safeguarding Lead and passed onto the Assistant Head (Pastoral and Boarding), the Deputy Head (Pastoral), and to the Senior Deputy, as required. Any issues will be followed up from an educational and/or disciplinary perspective.

Students are advised on what to do should they accidentally access inappropriate material and are expected to adhere to the Student Acceptable Use Policy and Boarding House Acceptable Use Policy as appropriate.

Students should ask the Director of IT for assistance if a website which is needed for school work has been blocked by the School's filtering system.

If a member of staff has any concern about the effectiveness of the filtering system, they must immediately report the matter to the Designated Safeguarding Lead in line with the School's Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to/or witnessed someone accessing harmful or inappropriate content. Teaching staff should notify the Director of IT if any appropriate teaching materials is being blocked.

5.2.2 Appropriate monitoring

As part of the School's safeguarding duties and in line with the School's Privacy Notice, the School monitors user activity and follows advice from the UKSIC guidance Appropriate Monitoring in Schools and the DfE Digital and Technology Standards for Schools/Colleges in doing so.

The management of the School's monitoring system is assisted by two external agencies, who monitor online content violations and reports serious concerns directly to the Director of Safeguarding/DSL who will put suitable safeguarding interventions in place as appropriate.

Technical monitoring is complemented by effective supervision in the classroom.

6. Procedures for responding to incidents of misuse

Staff, students and parents/carers are encouraged to report concerns, incidents of misuse or suspected misuse swiftly to allow the School to deal with them quickly and sensitively following the School's safeguarding and disciplinary policies and procedures.

The School recognises the importance of acknowledging, understanding and not downplaying behaviours which may be related to abuse and has appropriate systems in place to ensure that pupils can report any incidents of abuse, whether or not they include an online element, confidently and safe in the knowledge that their concerns will be treated seriously.

If a member of staff discovers that a student is at risk as a consequence of online activity, they should report it to the Director of Safeguarding/DSL as soon as reasonably possible who may seek assistance from the [CEOP](#) Safety Centre or other professional advisors as appropriate.

- Anti-Bullying Policy
- Values, Recognition and Conduct Policy
- Student Acceptable Use Policy
- Staff Code of Conduct

- Staff and Visitor Acceptable Use Policy

6.1 Misuse by students

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with the School's Safeguarding and Child Protection Policy and Values, Recognition and Conduct Policy

Whitgift School will not tolerate illegal activities or activities that are in breach of the this policy or the policies referred to above. Where appropriate the School will report illegal activity to the police and/or local safeguarding partnerships.

If the School reasonably suspects an electronic device has been, or is likely to be, used to commit an offence or cause harm, personal injury or damage to property, they may examine any data or files on the device where there is a good reason to do so and in line with the School's Searching a Student Policy. This may extend to online accounts, depending on the concern or the likelihood of potential harm.

6.1.1 Cyberbullying incident

Bullying by text, electronic messaging, e-mail, phone call, or social media can be highly intrusive and hurtful. The School strictly enforces its policies regarding the use of mobile phones and the internet and monitors closely all online communications on its network.

Students should be aware of the impact of cyberbullying and know how to seek help if they are affected by it. The Designated Safeguarding Lead or any other member of staff they trust, as well as parents and peers should be approached for advice or help if they experience problems when using the internet and related technologies.

Should a parent feel that their child is involved in cyberbullying, they should report it as soon as possible to the relevant Head of Year or the Director of Safeguarding/DSL.

Where any form of cyberbullying involves another student, whether the bullying or that student is in the School or another school, or may bring the School into disrepute, the School reserves the right to be involved. This applies whether the electronic material was produced within the School or outside.

Cyberbullying incidents, including incidents that take place outside school or from home, will be dealt with in accordance with the School's Anti-Bullying Policy and Values, Recognition and Conduct Policy. Students must be aware that some forms of cyberbullying are illegal and the School will inform the police when necessary.

6.1.2 Radicalisation

Radicalisation is the process by which individuals or groups come to adopt extreme views on political, religious and social matters, notably with the result of violent extremism. The School has a responsibility to protect students from extremist views, and to equip them with the ability to recognise, question and resist any attempts to radicalise them, especially during their formative years.

The internet has made it much easier for radicalisers to find and identify people who might be easily influenced and drawn into extremist behaviour. Anyone can be susceptible to being radicalised regardless of their age, but young people can sometimes be at greater risk.

One function of the school's monitoring is to identify those wishing to radicalise others. In addition, the Ideatum curriculum: educates students on how to recognise these attempts; promotes critical thinking; and suggests how students can seek support or raise any concerns they may have.

Anyone in the School community should bring to the School's attention any attempt to promote violent extremism, as a safeguarding concern, contacting the Designated Safeguarding Lead (DSL) or the Deputy DSL responsible for Prevent.

6.1.3 Responding to nudes and semi-nudes incidents (sexting)

The production and distribution of sexting images involving anyone under the age of 18 is illegal and needs very careful management for all those involved.

Staff **must never view, copy, print, share, store or save the imagery, or ask a child to share or download – this is illegal.** If staff viewed the imagery by accident (e.g. if someone has shown it to you before you could stop them), report this to the DSL (or equivalent) and seek support. Staff must immediately report any incident to the Director of Safeguarding/DSL who will then follow the UKCIS guidance Sharing Nudes and Semi-Nudes: [How to Respond to an Incident](#) which can be found in Appendix 1. Staff should also refer to the School's Searching a Student Policy. Incidents may include the sharing of digitally manipulated or AI-generated images.

The sharing of nudes or semi-nudes may constitute a criminal offence and will be considered in accordance with the School's Safeguarding and Child Protection Policy as well as the advice published by the UK Council for Child Internet Safety (UKCIS): [Sharing Nudes and Semi-Nudes: Advice for Education Settings Working with Children and Young People](#).

It is important that everyone understands that whilst the sharing of nudes and semi-nudes is illegal, students can come and talk to members of staff if they have made a mistake or had a problem in this area.

6.1.4 Use of AI and deepfake technology

The use of Artificial Intelligence (AI), including generative tools and deep fake technology, presents both opportunities and risks in the context of online safety and safeguarding. In accordance with *Keeping Children Safe in Education (KCSIE) 2026*, this school recognises the emerging risks associated with AI-generated content, including:

- The potential for **misinformation, disinformation, and conspiracy content**, which may influence pupils' worldviews and online behaviour;
- The creation and spread of **deep fake images, videos, or audio** that may be used to bully, harass, deceive, or manipulate others;

- The misuse of **AI tools to generate inappropriate or harmful material**, including sexually explicit, violent, or extremist content.
- AI-generated nudification images;
- Synthetic sexual imagery and image-based abuse;
- AI-enabled impersonation and identity fraud;
- Manipulation through AI chatbots and virtual companions;
- AI-assisted bullying, harassment and coercion.

The School recognises that AI technologies evolve rapidly and that new forms of AI-enabled harm may emerge. Consequently, staff should exercise professional curiosity and report concerns where technology appears to have contributed to safeguarding risk, even where the precise technology involved is unclear.

If staff have any concerns about a child in this area, they should refer the matter to the Director of Safeguarding/DSL immediately. Any incidents involving the use of AI will be dealt with by the DSL as well as appropriate staff such as the relevant Director of Section, Assistant Head (Pastoral & Boarding) and the Deputy Head (Pastoral).

6.1.5 Cybercrime

Cybercrime is criminal activity committed using computers and/or the internet. It is broadly categorised as either 'cyber-enabled' (crimes that can happen offline but are enabled at scale and at speed online) or 'cyber dependent' (crimes that can be committed only by using a computer). Sextortion (**Threats to share sexual images or videos** of a person unless they meet certain demands such as money, more images, or further communication) is also considered a cyber crime. If a member of staff receives a disclosure, or comes to learn that sextortion has taken place, they must report it to the DSL immediately.

The School is aware that students with particular skill and interest in computing and technology can be at risk of straying into cyber-dependent crime.

If staff have any concerns about a child in this area, they should refer the matter to the Director of Safeguarding/DSL immediately who might consider a referral into the Cyber Choices programme, a nationwide police programme supported by the Home Office and led by the National Crime Agency.

6.2 Misuse by staff

If anyone has a safeguarding-related concern relating to staff misuse of technology, they must report it immediately in accordance with the School's procedures on raising concerns and dealing with allegations which is set out in the School's Safeguarding and Child Protection Policy.

Any other unsuitable activity or access to unsuitable materials should be reported in accordance with the School's Low Level Concerns Policy as appropriate.

7. Safe use of digital technology and communication

The School's acceptable use policies, Staff Code of Conduct as well as Social Media and Communication Policy set out the School rules about the use of digital technology

and communication including internet, email, social media and mobile electronic devices, helping students and staff to protect themselves and others when using technology.

Students are reminded of the importance of the Student's Acceptable Use Policy and Mobile Devices Acceptable Use Policy on a regular basis.

As most Whitgift boarders are on site full time, the School acts also as their term-time home. This means that there are additional opportunities available to them through the Founder's House wi-fi system. These include both educational and recreational use of the internet, the opportunity to communicate with their families through Teams, Zoom, Facetime or similar services. As a result of this, there are specific protocols for online use in Founder's House, as outlined in the Boarding House Acceptable Use Policy. Students should note that they are also bound to observe the terms of this policy.

The aspects of the curriculum relating to safe use of technology are reviewed on a regular basis to ensure their relevance.

7.1 Communication between staff and students/parents

Any digital communication between staff and students or parents must be professional in tone and content. All staff should maintain an appropriate relationship between themselves, students and parents and in accordance with the School's Staff Code of Conduct, Staff and Visitor Acceptable Use Policy as well as the Social Media and Communications Policy.

For communication with students, staff should only use systems that are under the regulation of the School network. This is for the mutual protection and privacy of all staff, students and parents, supporting safeguarding best-practice. Currently, this is restricted to:

- the School's email system (Outlook),
- Firefly messaging service,
- Microsoft Teams.

The School recognises though that there are situations (for example in emergencies) where there may be no alternative.

Should a member of staff wish to discuss a concern on the use of digital communication, they should seek the advice of the Director of Safeguarding/DSL, the Senior Deputy or any other senior colleague.

Any accidental use of personal email address or telephone number to communicate with students or parents should be reported in line with the School's Low-Level Concerns Policy.

7.2 Professional standards for the use of social media

Staff should be aware of the potential audience of any social media services that they use in their professional or private capacity, maintaining the same expected standards of professionalism, as befitting the position of trust of anyone working in the School.

They must adhere to the standards outlined in the School's Social Media and Communications Policy, Staff and Visitor Acceptable Use Policy as well as the Staff Code of Conduct.

7.3 Safe use of digital images

Staff, parents and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. Staff should inform and educate students about the risks associated with the taking, using, sharing, publication and distribution of images and encourage students to think about their online reputation and digital footprint.

Staff should only use images of students where permission has been obtained, and only for the given purpose.

Photographs chosen to be published on the School's social media platforms and school website must be selected carefully and must never identify a student by full name without specific permission. Please refer to the school's Taking, Storing, Using Images Policy for further information.

Staff, students and parents are reminded of the importance of not sharing without explicit permission, due to reasons of child protection, data protection, religious or cultural reasons, or simply for reasons of personal privacy.

8. Risk assessment

The School recognises that technology, and the risks and harms associated with it, evolve and change rapidly. The School will carry out regular reviews of its approach to online safety (including filtering and monitoring), supported by risk assessments which consider and reflect the risks faced by the students.

Where a concern about a student's welfare is identified, the risks to that student's welfare will be assessed and appropriate action be taken to reduce the risks identified. The School recognises that online experiences can significantly affect a child's emotional wellbeing and mental health. Exposure to harmful content, cyberbullying, online exploitation, social comparison, image manipulation, harmful communities and excessive technology use may contribute to anxiety, emotional distress, self-harm, eating difficulties and other mental health concerns.

The format of the risk assessment may vary and may be included as part of the School's overall response to a welfare concern, including the use of individual student welfare plans as appropriate. Risk assessment may draw upon safeguarding data, incident trends, student voice, pastoral information, filtering and monitoring data, local context and national guidance. Regardless of the form used, the School's approach to promoting the student welfare will be systematic and student focused.

9. Record keeping

All serious incidents and investigations involving the use of technology will be centrally logged and kept as part of the student or staff record.

The information created in connection with this policy may contain personal data. The School's use of personal data will be in accordance with data protection law and in line with the School's data protection policies and procedures. The School has published privacy notices which explain how the School will use personal data.

Appendix 1 : Sharing Nudes and Semi-Nudes: How to Respond to an Incident

The below guidance is intended for staff. Safeguarding staff should refer to the full UKCIS guidance.

Sharing nudes and semi-nudes: how to respond to an incident

An overview for all staff working in education settings in England

UK Council for
Internet Safety

This document provides a brief overview for frontline staff of how to respond to incidents where nudes and semi-nudes have been shared.

All such incidents should be immediately reported to the Designated Safeguarding Lead (DSL) or equivalent and managed in line with your setting's child protection policies.

The DSL or equivalent should refer to the full 2024 guidance from the UK Council for Internet Safety (UKCIS), [Sharing nudes and semi-nudes: advice for education settings working with children and young people](#), for managing incidents.

What do we mean by sharing nudes and semi-nudes?

In the latest advice for education settings (UKCIS, 2024), this is defined as the sending or posting of nude or semi-nude images, videos or live streams online by young people under the age of 18. Nudes and semi-nudes can be shared online via social media, gaming platforms, chat apps, forums, or involve sharing between devices using offline services. Alternative terms used by children and young people may include 'dick pics' or 'pics'. The motivations for taking and sharing nude and semi-nudes are not always sexually or criminally motivated.

This advice does not apply to adults sharing nudes or semi-nudes of under 18-year olds. This is a form of child sexual abuse and must be referred to the police as a matter of urgency.

What to do if an incident comes to your attention

Report it to your Designated Safeguarding Lead (DSL) or equivalent immediately. Your setting's child protection policy should outline codes of practice to be followed.

- **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.¹
- If you have already viewed the imagery by accident (e.g. if someone has shown it to you before you could stop them), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

¹ In exceptional circumstances, it may be necessary for the DSL (or equivalent) only to view the image to safeguard the child or young person. That decision should be based on the professional judgement of the DSL (or equivalent).

[Sharing nudes and semi-nudes: how to respond to an incident \(overview\) \(updated March 2024\) - GOV.UK](#)
[Sharing nudes and semi-nudes: advice for education settings working with children and young people \(updated March 2024\) - GOV.UK](#)