



Wellington College

Document Control

Title of Policy:	Online Safety Policy (including mobile phone use policy and remote learning guidance)
Policy/Procedure Owner:	Director of Safeguarding & Deputy Head Pastoral (Mobile Phone Policy)
Date Last Reviewed:	September 2026
Date of Next Review:	September 2027
Ratified by Governors:	September 2026

Background and Rationale

Safeguarding young people at Wellington College is taken very seriously. In the College Safeguarding and Child Protection policy it is clear that as a school we are committed to “creating and sustaining a safe learning environment” and identifying that “where there are child welfare concerns, we will take action to address them.” All staff at Wellington College are trained to understand and appreciate that everyone has a duty to safeguard and promote the welfare of children – and not just those at Wellington College.

Keeping Children Safe in Education (2026) defines safeguarding as “protecting children from maltreatment whether inside or outside the home, including online; preventing impairment of children’s mental and physical health or development; ensuring that children grow up in circumstances consistent with the provision of safe and effective care; and taking action to enable all children to have the best outcomes.” The requirement to ensure that children and young people are able to use the internet and related communication technologies appropriately and safely is a vital part of the wider duty of care to which all who work at Wellington College are bound.

A school online safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all the individuals in a child’s education from the Master and Governors to the Executive Leadership Team and classroom teachers, non-teaching staff, parents, members of the community and, most importantly, the students themselves.

New technologies have become integral to the lives of children and young people in today’s society, both within schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. However, it must also be remembered that children and young people have an entitlement to safe internet access at all times.

Whilst the use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include (KCSIE 2026):

Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.

Contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes’.

Conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography) including AI-generated explicit images, deepfake

imagery and AI generated nudes or semi-nudes, sharing other explicit images and online bullying; and

Commerce - risks such as online gambling, inappropriate advertising, phishing¹ and or financial scams.

Whilst the use of digital technologies provides significant educational, social and creative opportunities, it also exposes children and young people to an evolving range of safeguarding risks. Online harm can occur through the sharing of inappropriate content, harmful contact with others, unsafe online conduct or commercial exploitation. Increasingly, these risks include the misuse of artificial intelligence (AI), such as AI-generated or manipulated images (including deepfakes and AI-generated nudes or semi-nudes), misinformation and disinformation, online fraud, and technology-facilitated abuse. The College recognises that safeguarding incidents rarely occur solely online or solely offline; in many cases, abuse and exploitation take place concurrently across both environments. Wellington College therefore adopts a whole-school approach to online safety, ensuring that online safeguarding is fully integrated within its wider safeguarding culture, policies, procedures and curriculum so that pupils are supported to recognise risks, build resilience, report concerns and use technology safely, responsibly and respectfully.

Many of these risks reflect situations in the off-line world and it is essential that this online safety policy is used in conjunction with other school policies:

- Behavioural Policy
- Child-on-child abuse policy
- Safeguarding policy
- Acceptable Use Policy (AUP)
- Social media policy
- Artificial Intelligence policy
- Filtering and monitoring policy

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Wellington must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of them to manage and reduce these risks. Underpinning the following online safety policy are the frameworks and Government legislation set out in:

- Keeping Children Safe in Education (2026)
- Working together to Safeguard Children (2018, updated 2026)
- Meeting Digital and Technology Standards in Schools and Colleges' (DfE, 2023)
- Sharing of nudes and semi-nudes: advice for education settings working with children and young people (DfE 2020, updated March 2024)
- Generative artificial intelligence (AI) in education (DfE, June 2025)

¹ If students or staff are at risk, reports can be made to the Anti-Phishing Working Group (<https://apwg.org/>)

- The Online Safety Act (July 2025)
- Safeguarding and Remote Education (DfE, 2022)
- Providing Remote Education (DfE, 2024)

In June 2025, the DfE published detailed guidance and policy papers outlining expectations and best practices for the safe and effective use of AI in education settings.² Further detail on responding to AI-generated child sexual abuse material, please see Appendix 6. All staff are expected to be familiar with the DfE guidance.

The policy that follows explains how we intend to manage the risks mentioned above, while also addressing wider educational issues in order to help young people (and their parents) to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

In 2023, the College was recognised as a National Online Safety Certified School, and all teaching staff completed the National College's 'Certificate in Online Safety.'

Development / Monitoring / Review of this Policy

This Online safety policy has been reviewed by:

- Director of Safeguarding (Designated Safeguarding Lead)
- Deputy Head (Pastoral)
- Assistant Head (Pupils)
- Safeguarding Manager
- Director of IT Services and Development
- Director of Digital Learning
- Director of Legal and Compliance

Information regarding the policy is shared with the whole school community through the following:

- Staff meetings and the College SharePoint site
- Weekly safeguarding emails
- Governors' meeting / subcommittee meeting (Pastoral and Safeguarding subcommittee)
- College safeguarding website
- The Week Ahead newsletters and Safeguarding newsletters for parents
- Information sharing via the Parental Online Committee

The policy will be reviewed annually by the Governors alongside the Safeguarding policy. The College also enjoys strong links with Bracknell Forest Local Children's Safeguarding Board and the policy will also be sent annually to the Bracknell Forest Safeguarding Our Schools Team. Any changes to the policy (due to legislation changes or in light of any significant new developments

² <https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education/generative-artificial-intelligence-ai-in-education>

in the use of technologies, new threats or online safety incidents that have taken place) will be clearly identified.

Should any serious incidents take place, the Designated Lead for Safeguarding will be informed and communication with Children's Social Care or the LADO if appropriate.

Scope of the Policy

This policy applies to all members of the Wellington community (including staff, students, volunteers, parents, visitors) who have access to and are users of school ICT systems, both in and out of school.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school. This may include, for example, instances of where cyber bullying has taken place over the summer holidays and has continued into term time or if a pupil has brought the school into disrepute over social media using a personal device, or from their home.

The school will deal with such incidents within this policy and associated behaviour, child-on-child abuse and sexual harassment policies and will, where known, inform parents of incidents of inappropriate online safety behaviour that take place out of school.

Additional information about cyberbullying can also be found in the child-on-child abuse policy and online safety advice and resources can be found in KCSIE 2026³.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the school:

The Governors, Master and ELT

- The Master is responsible for ensuring the safety of the members of the school community, though the day-to-day responsibility for online safety will be delegated to the Deputy Head (Pastoral), Director of Safeguarding and the Safeguarding Manager
- The Master and the ELT are responsible for ensuring that the relevant staff receive suitable CPD to enable them to carry out their online safety roles and to train other colleagues, as relevant
- The Master and the ELT 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The TLT will also review any online safety incidents and discuss them, addressing what had been done well and what could have been done better. In accordance with the College ethos, an undefended and reflective approach will be taken.

³ <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>

- Should a member of staff need any support following an online safety incident, the ELT will ensure that appropriate support be given to that individual and confidential counselling offered if needed.

The Governors and ELT should also:

- Receive assurance that filtering and monitoring are effective.
- Review reports on online safety risks and mitigation.
- Ensure sufficient resources are available to maintain effective systems.
- Challenge the Director of Safeguarding and Director of IT where arrangements require improvement.

Leadership of Online Safety

The Director of Safeguarding takes responsibility for online safety within the College. They liaise closely with the Deputy Head (Pastoral) and the Safeguarding Manager who will advise on the pastoral aspects of online safety and the education of online safety within the College (through the Well- being programme; assembly/tutorial programme and workshops). They will meet at least twice termly with the Director of IT Services and Development and the Second Master to look at any aspects of online safety that need to be addressed, however it is expected that informal liaison will take place on a much more regular basis and as and when required. The Director of Safeguarding will:

- Act as main point of contact on online safety issues and liaise with other members of staff as appropriate.
- Ensure policies and procedures that incorporate online safety concerns are in place. This should include but is not limited to; Safeguarding policy; Acceptable Use Policies (AUPs), mobile phones, child on child abuse (including responses to cyberbullying and sexting/youth produced imagery), filtering and monitoring and social media.
- Ensure there are robust reporting channels (via MyConcern) and signposting to internal, local and national support.
- Ensure filtering and monitoring arrangements are considered as part of the College's safeguarding arrangements.
- Work with the Director of IT Services and Development to review the effectiveness of filtering and monitoring at least annually.
- Ensure concerns identified through monitoring are assessed from a safeguarding perspective and acted upon appropriately.
- Ensure staff understand how to report concerns arising from filtering and monitoring.
- Report significant findings and emerging risks to the ELT and Governors.
- Ensure records of safeguarding actions arising from monitoring are maintained.
- Record online safety incidents and actions taken, in accordance with Wellington College Safeguarding policy.
- Ensure the whole school community is aware of what is safe and appropriate online behaviour (using the Headstart Kernow Digital resilience tool)⁴ and understand the sanctions for misuse.

⁴ <https://www.headstartkernow.org.uk/for-prof/digital-resilience/>

- Liaise with the local authority and other local and national bodies as appropriate.
- To lead an online safety group (which includes a member of teaching staff who leads on the education of online safety; the Director of IT and a member of IT staff who leads on online safety), who will work together to develop an online safety curriculum and inform technical decisions and monitoring. To facilitate regular meetings of the group who will steer and implement tasks such as (but not limited to):
 - Producing and reviewing policies
 - Mapping, planning and reviewing the online safety curriculum
 - Producing, reviewing and monitoring the school monitoring and filtering policy
 - Consulting with stakeholders
 - Raising awareness throughout the community
 - Auditing online safety practice and policy compliance
 - Creating and implementing an online safety action plan
 - Reporting regularly to the governing body to help inform them of existing practice and localised concern
- Keep the Second Master regularly informed of any incidents and concerns and take responsibility for implementing actions as appropriate liaising with the Assistant Head (Pupils) over disciplinary decisions.
- Work with the Director of IT Services and Development to ensure that filtering and monitoring systems are appropriate, effective and reviewed at least annually. Ensure records of these reviews are maintained, that all internet-enabled devices used within the College are included within filtering and monitoring arrangements where appropriate, and that safeguarding concerns identified through monitoring are assessed promptly and acted upon in accordance with the College's safeguarding procedures.
- Take appropriate action in line with child protection policies and procedures, if the filtering system and monitoring approaches identify any causes for concern. Work with the College Legal and Compliance Director to ensure that online practice is in line with current GDPR legislation
- Implement regular online safety training for all members of staff (including as part of induction) that is integrated, aligned and considered part of the overarching safeguarding approach (KCSIE 2026).
- Work with staff to ensure that appropriate online safety education is embedded throughout the curriculum; promoting the responsible use of technology and empowering children to keep themselves and others safe online.
- Actively engage with local and national events to promote positive online behaviour, e.g. Safer Internet Day and anti-bullying week.
- Update the College online safety risk assessment on an annual basis in conjunction with the Director of IT and Director of Digital Learning
- Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches, including the Wellington College Parent's online safety group
- Ensure that their own knowledge and skill are refreshed at regular intervals to enable them to keep up to date with current research, legislation and trends. To understand the unique risks associated with online safety and be confident that they have the relevant

knowledge and up to date capability required to keep children safe whilst they are online at school or college; can recognise the additional risks that children with SEN and disabilities (SEND) face online, for example, from online bullying, grooming and radicalisation and are confident they have the capability to support SEND children to stay safe online.

- Evaluate the delivery and impact Wellington College's online safety policy and practice
- Review any reported online safety incidents to inform and improve future areas of teaching, training and policy development
- Feedback online safety issues to the management/leadership team and other agencies, where appropriate

The Director of Safeguarding has responsibility for online safety within the school and should be trained in online safety issues (including understanding the filtering and monitoring systems and process in place) and be aware of the potential for serious child protection issues to arise from:

- Sharing of personal data
- Access to illegal / inappropriate materials
- Inappropriate on-line contact with adults / strangers
- Potential or actual incidents of grooming
- Online bullying
- Liaise with Children's Social Care and the LADO when appropriate

The Director of Safeguarding has regular meetings with the DSL team in order to keep the safeguarding team abreast of online safety issues both nationally and within the College.

Student involvement and voice

The College acknowledges, learns from, and uses the skills and knowledge of learners in the use of digital technologies. We recognise the potential for this to shape the online safety strategy for the College community and how this contributes positively to the personal development of young people. Their contribution is recognised through the student-led committees within the College and specifically through the junior student voice group – "Prisms". Students annually take the lead on Safer Internet day working alongside the staff online safety committee. More information about student participation can be found in the Online Safety risk assessment.

The Director of IT Services and Development / IT staff

The Director of IT Services and Development and the College IT Services Department are responsible for ensuring:

- That the school's ICT infrastructure is secure and is not open to misuse or malicious attack
- That users may only access the school's networks through a properly enforced password protection policy, in which passwords are regularly changed
- The school's filtering and monitoring policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- Implement and maintain appropriate filtering and monitoring systems.
- Undertake regular testing (at least on an annual basis) to ensure systems remain effective.

- Keep records of testing, system reviews and technical changes.
- Ensure filtering and monitoring apply to all relevant internet-connected devices and networks.
- Work with the DSL to review the effectiveness of arrangements annually.
- Ensure the College meets the DfE Filtering and Monitoring Standards.
- That they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That the use of the network / Virtual Learning Environment (VLE) / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Director of Digital Learning for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in school policies
- That they liaise with the Director of Digital Learning reporting any concerns

Teaching and Support Staff

The teaching and support 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 including an understanding of the filtering and monitoring processes in place
- They have read, understood and signed the school Staff Acceptable Use Policy (AUP) and the online safety policy
- They report any suspected misuse or problem (for example failure to comply with the conditions of the AUP) to the Director of Safeguarding or Deputy Head (Pastoral) for investigation / action / sanction (any decision of which will be made in conjunction with the Second Master)
- Digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other school activities
- Understand their role in filtering and monitoring arrangements and know how to escalate concerns identified through monitoring systems.
- Students understand and follow the school online safety and Staff Acceptable Use Policy
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor ICT activity in lessons, extra curricular and extended school activities, recognising that students using mobile phones may be using their own data access and not the college Wi-Fi.
- They are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices, especially with regard to students using their own data plans to access the internet.
- In lessons where internet use is pre-planned students 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
- They celebrate the positive use of ICT and digital media and promote correct usage

Students

- Are responsible for using the school ICT systems in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to school systems.
- Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- 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 school policies on the use of mobile phones, digital cameras and handheld devices. They should also know and understand school 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 and realise that the school's online safety policy covers their actions out of school, if related to their membership of the school

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Research shows that many parents and carers do not fully understand the issues and are less experienced in the use of ICT than their children. The school will therefore take every opportunity to help parents understand these issues through parental masterclass talks, advice in the Week Ahead, letters home, the College website and information about national / local e-safety campaigns / literature.

Parents also need to be aware that if their children are supplied with a 3G/4G/5G mobile device will be able to access the internet independently of the College system and therefore the College blocking and filtering system will not operate. This further highlights the need for parents and carers to take responsibility for educating their own children in the area of digital technology and social media alongside the work that the College undertakes.

Parents and carers will be responsible for:

- Ensuring that they are well – educated themselves on all matters of online safety. Parents are strongly encouraged to engage with the support material that the College provides over the course of the academic year
- Supporting the College actions where an e-safety incident has been dealt with
- Accessing the school website / VLE / on-line student / pupil records in accordance with the relevant school Acceptable Use Policy

Education and Training

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to learn about online safety and to recognise and avoid online safety risks and build their resilience.

Online Safety education will be provided in the following ways:

- All pupils will sign the Acceptable Use Policy at the start of each academic year
- A planned online safety programme is provided as part of the Well-being curriculum. In addition to this key online safety messages will be reinforced to each year group through assemblies, tutorials and workshops as part of the College's Relationships Education programme. The content of lessons and talks will be regularly reviewed so that they are up to date and relevant. Content includes explicit teaching around AI generated images, deepfakes, manipulated images, misinformation created using AI, online coercion using AI and recognising AI generated scams.
- The DSL will, through start of year talks, highlight the issue of sexting to all pupils so that they are fully aware of the legal implications of images and the fact that the image may be considered indecent.
- Students should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students should be helped to understand the need for the student AUP and encouraged to adopt safe and responsible use of ICT, the internet and mobile devices both within and outside school. They should also be educated about protecting their own devices (such as password protecting their mobile and tablets).
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Staff should act as good role models in their use of ICT, the internet and mobile devices.

Education – parents

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- The Week Ahead
- Termly safeguarding newsletter
- The Wellbeing Hub
- Talks run by the College in all matters of online safety, including mobile phone use

Education & Training – Staff

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff have read the College online safety policy
- All staff and their families (who have access to the College network) have read and signed the Acceptable Use Policy

- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety policy, Acceptable Use Policies and the filtering and monitoring systems in place.
- All staff have access to the National College training platform in order to keep abreast of up-to-date information on online safety issues.
- The Director of Safeguarding will provide advice / guidance / training as required to individuals as required e.g. through the safeguarding weekly emails, safeguarding newsletters and National College platform.

Training – Governors

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any group involved in ICT / online safety / health and safety / child protection. This may be offered by:

- Safeguarding Governor training
- Participation in school training / information sessions for staff
- Membership and access to National College courses/guides/webinars

Incident Management Procedures

The College will take all reasonable precautions to ensure online safety for all College users but recognises that incidents may occur inside and outside of the College (with impact on the College) which will need intervention. The College will ensure:

- there are clear reporting routes which are understood and followed by all members of the College community which are consistent with the College safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies. At Wellington College, we use online/anonymous reporting systems SWGfL Whisper
- all members of the College community will be made aware of the need to report online safety issues/incidents
- reports will be dealt with as soon as is practically possible once they are received
- the Designated Safeguarding Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
 - if there is any suspicion that the incident involves any illegal activity or the potential for serious harm (see flowchart and user actions chart in Appendices 3 and 4), the incident must be escalated through the agreed College safeguarding procedures, this may include:
 - Non-consensual images
 - Self-generated images
 - Terrorism/extremism
 - Hate crime/ Abuse
 - Fraud and extortion
 - Harassment/stalking
 - Child Sexual Abuse Material (CSAM)
 - Child Sexual Exploitation Grooming
 - Extreme Pornography
 - Sale of illegal materials/substances
 - Cyber or hacking offences under the Computer Misuse Act

- Copyright theft or piracy
- any concern about staff misuse will be reported to the Master, unless the concern involves the Master, in which case the complaint is referred to the Chair of Governors and the local authority.
- it is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively
- there are support strategies in place e.g., peer support for those reporting or affected by an online safety incident
- incidents should be logged in MyConcern (students) and Confide (staff)
- relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g., local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions (as relevant)
- learning from the incident (or pattern of incidents) will be provided (as relevant and anonymously) to:
 - the Online Safety Staff Group for consideration of updates to policies or education programmes and to review how effectively the report was dealt with
 - staff, through regular briefings
 - learners, through assemblies and wellbeing lessons
 - parents/guardians, through newsletters and correspondence home
 - governors, through regular safeguarding updates

Any incident of child-on-child online abuse will be dealt with through the Child-on-child abuse, behavioural and incident management policies.

Technical – infrastructure / equipment, filtering and monitoring

The College will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. The College will also ensure that it meets the standards as laid out in the DfE document 'Meeting digital and technology standards in schools and colleges' (March 2023).

The Director of Safeguarding will work collaboratively with the Director of IT Services and Development and other relevant members of the Senior Leadership Team to ensure that the College's filtering and monitoring arrangements remain appropriate, proportionate and effective. The effectiveness of these arrangements will be formally reviewed at least annually, and more frequently where changes in technology, safeguarding risks or incidents indicate that this is necessary. Reviews will consider the effectiveness of filtering and monitoring across all relevant internet-enabled devices, networks and platforms used within the College, taking account of the Department for Education's Filtering and Monitoring Standards, *Plan Technology for Your School* guidance and relevant guidance relating to the safe use of generative artificial

intelligence in education. Appropriate records of reviews, testing and actions taken will be maintained. All staff will receive regular training on the College's filtering and monitoring arrangements, understand their individual responsibilities, and know how to recognise and report safeguarding concerns identified through these systems in accordance with the College's safeguarding procedures.

The College will also need to ensure that the relevant people named in the above sections will be effective in carrying out their online safety responsibilities:

- There will be regular reviews and audits of the safety and security of school ICT systems. This will be covered in meetings between the Director of Safeguarding and the Director of IT Services and Development. These audits and any action points will be shared with the ELT
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be recorded by the Director of IT Services and Development and will be reviewed, at least annually, by the Director of Digital Learning
- All users will be provided with a username and password by IT Services who will keep an up to date record of users and their usernames. Users will be required to have a robust password
- Users will be made responsible for the security of their username and password, 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.
- The school has provided enhanced user-level filtering through the use of the Palo Alto filtering programme. The specific software used for this process is kept under review as other products and systems become available.
- In the event of the Director of IT Services and Development needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Master or the Director of Safeguarding.
- Requests from staff for sites to be removed from the filtered list will be considered by the Director of Safeguarding and the Deputy Head (Pastoral).
- School IT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy. Monitoring will take place monthly using a random sample of students. The activity of specific students may be monitored if advised by an individual's HM and permission sought through the Director of Safeguarding.
- Each month, the Director of IT Services and Development will randomly sample 10 staff to student emails (this should include all staff, not just teaching staff)
 - A confidential record is to be kept of which emails have been sampled.
 - Emails will be read to and checked for:
 - General inappropriate language – overtly disciplinarian or affectionate. Anything which suggests an uncomfortable power imbalance between the adult and the child such as threatening or intimidating language or

anything which suggests a relationship which might be too close such as flirtatious language.

- Pupil language – general email etiquette and the way in which they are engaging with the member of staff. All email contact needs to be ‘professional’. All emails should be professional in their tone and content.
 - Inappropriate conduct – including personal mobile phone numbers, personal email details or home address or social media contact details. Organising to meet a pupil in an inappropriate place / time. Same to be looked for in pupil emails. Anything which would go against the safeguarding policies in the school or the AUP.
 - Wider context – has an email been sent when a different method of communication would have been better? Is there some education to be done with staff / pupil.
- Should there be no concerns, the Director of IT Services and Development will write a short report based on his findings to be sent to the College DSL. This should include any general trends which might have been spotted, or simply a sentence indicating that there were no concerns. The report should include the time / date of sampling and the sampling method used as well as a general statement about the year groups sampled.
 - If a minor concern is picked up about an individual, this should be shared with the DSL immediately and this will be addressed. It is likely to be treated as a low-level concern and the individual spoken to directly and educated.
 - If a major safeguarding concern is picked up, this should be shared with the DSL immediately and will be dealt with in accordance with the College safeguarding policies and procedures.
 - Three times a year the DSL will go through the checking process with the Director of IT Services and Development in order to ensure that the guidance is being followed and that important information is not being missed.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, handheld devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.
 - The school infrastructure and individual workstations are protected by up to date virus software.
 - Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
 - Monitoring of student’s online activity is fulfilled through the use of Lightspeed. The efficacy of this system is tested half termly by the Safeguarding Manager as part of the filtering and monitoring policy

Curriculum

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages in the use of ICT across the curriculum.

- In lessons where internet use is pre-planned, it is best practice that students 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
- Where students are allowed to freely search the internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit by continually moving around the classroom and engaging with the pupils throughout the lesson and to be aware that students may be using mobile data to access the internet.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Director of IT Services and Development can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should also be cleared with the Director of Safeguarding.
- Students should be taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information, with particular focus on scamming and changes in cyber-crime.
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. There are many reported incidents of employers carrying out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites
- Staff are allowed to take digital / video images to support educational aims, but must follow school safeguarding policy concerning the sharing, distribution and publication of those images. Those images should be taken on school equipment, the personal equipment of staff should not be used for such purposes. If a member of staff wants to use their own equipment, they need the permission of the Deputy Head (Pastoral).
- Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute. If in doubt, the individual should ask the advice of the Deputy Head (Pastoral).
- Students must not take, use, share, publish or distribute images of other pupils without their permission. It must be recognised by the students that these permissions can change depending on the relationship between particular groups of students.

- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images. The College's Terms and Conditions clarifies what is permissible and parents are required to opt out of the sharing of such images when signing the College contract. Any images which are published should be without the name of the individual pupil (unless permission has been agreed by the pupil and their parent).
- Particular care should be taken in subjects such as Art, where it may be necessary for students to capture images using digital media of semi-naked models as part of their portfolio work. Advice should be sought from the DSL for safeguarding if there are any concerns. The Art department has its own code of conduct for artists and photographers.
- Student's work can only be published with the permission of the student

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Staff must ensure that they are fully conversant with the College Data Protection policy. In the context of e-safety, they should particularly:

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- It is good practice to password protect the device
- The device must offer approved virus and malware checking software
- The data must be securely deleted from the device, once it has been transferred or its use is complete

Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following list shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

Appropriate activities/Good practice

When using communication technologies, the school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature to the Second Master. Users can also report such an incident using the Whisper (confidential reporting app) which is monitored by the Director of Safeguarding, Safeguarding Manager Deputy Head Pastoral. The recipient must not respond to any such email. If the recipient is a pupil, they should inform any member of staff although it is likely that they will speak to their HM in the first instance. The email should be printed and saved before any further action is taken by the Second Master
- Any digital communication between staff and students or parents must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Information on the College social media sites will be uploaded by the designated member of staff and content is monitored by the Director of Safeguarding. They are also subject to the disciplinary procedures of the College and the Facebook and Twitter privacy policies.
- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.
- Personal information should not be posted on the school website, and only official email addresses should be used to identify members of staff.
- The College Safeguarding policy and staff code of conduct details the policy on the staff use of mobile phones.

Unsuitable / inappropriate activities

The school believes that the activities referred to in the following section would be inappropriate in a school context and that all users of the school IT system should not engage in any of the following activities in school or outside school when using school equipment or systems.

- Child sexual abuse images as laid out in statutory law⁵
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation
- Adult material that potentially breaches the Obscene Publications Act in the UK⁶
- Criminally racist material in the UK
- Pornography
- Promotion of any kind of discrimination, racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to another student or colleague, breaches the integrity of the ethos of the school or brings the school into disrepute
- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school

⁵ <https://www.cps.gov.uk/legal-guidance/indecent-and-prohibited-images-children>

⁶ <https://www.cps.gov.uk/legal-guidance/obscene-publications>

- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- Online gambling should not be used by any of the pupils in school or outside school when using school equipment or systems. It should be remembered that gambling is illegal under the age of 18.

Responding to incidents of abuse

It is assumed that all members of the school community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Any such incidents should be reported to the Director of Safeguarding or the Director of Digital Learning. All staff are reminded that there is a clear College Whistleblowing policy (accessed from the main policies link on MyDay) which they should refer to and students may also use Whisper to report concerns anonymously.

Remote learning

Where children are being asked to learn online at home the Department of Education has provided advice to support schools and colleges do so safely: [safeguarding and remote education](#). The college's remote teaching policy can be found in Appendix 11.

Reviewed October 2019 in line with KCSIE 2019
Reviewed Jan 2021 and changes made in line with KCSIE 2020 and remote learning
Reviewed Sept 2021, incorporated mobile phone policy and KCSIE 2021 changes
Reviewed by JCG Sept 2022, incorporated KCSIE 2022 changes, and updated remote learning
Reviewed by DAL Sept 2023, incorporated KCSIE 2023 changes and inclusion of DfE Filtering and Monitoring Standards
Reviewed by DAL Sept 2024 to include KCSIE 2024 changes
Reviewed by DAL Sept 2025 to include KCSIE 2025 changes, updated mobile phone policy, Appendices 3, 4, 5 and 6; Generative AI DfE guidance, Online Safety Act 2023
Reviewed by DAL Sept 2026 (changes made to reflect KCSIE 2026)

APPENDIX 1

Mobile Phone Policy for 2026-27

2026-27 Introduction

This policy forms part of the Filtering and Monitoring Policy and is consistent with our education for all pupils on digital use and safety. It also incorporates the current [June 2026] Government rules on the use of mobile phones during the teaching day and embeds anticipated rule changes around social media use for under-16s.

A policy of this nature has to strike a balance between compelling arguments on every side with close reference to other schools which, like Wellington College, operate a complex model of co-ed day, weekly and full boarding, all elements of which present a different emphasis in relation to the need, or otherwise, of mobile technology. Any policy on access to phones has to sit inside a wider consideration of device usage, as well as a robust package of education around digital use.

As part of this review, we have consulted staff, pupils, parents, similar schools to Wellington, recent research and the Boarding School's Association. This policy is ratified by the Executive Leadership Team.

Tom Wayman, Deputy Head (Pastoral)

Times

Year	Phones Allowed	All years to hand in phones overnight.
3 rd	19.00-19.25	No Smartphones ⁷ . In-House use only.
4 th	19.00-19.25	In-House use only.
5 th	18.00-19.25	
L6	16.30-19.25 21.00-22.00	
U6	16.30-22.00	U6 can request to keep phone overnight from January in agreement with parents and HM.

Notes

1. Other smart technology with similar functionality to a mobile phone is included in this policy.

⁷ Recommended 3rd form phones can be chosen from
<https://www.smartphonefreechildhood.org/alternatives#follow-on-phones> and
<https://www.smartphonefreechildhood.org/alternatives#first-phones>.

2. All pupils should bring in a payment card, watch and alarm clock. Parents are advised to speak with HMs if the payment card option is unsuitable (for any reason). Every House has a House Mobile which pupils may use if needed and parents can use to contact pupils and staff.
3. Where a pupil's or House Year Group's independent academic attainment, co-curricular participation and/or social wellbeing is a cause for concern, the Tutor and HM will review their phone use.
4. If the authorised timings clashes with another commitment, an equivalent time will be permitted in the day. Pupils who need to contact their family in a different time zone can agree a suitable time with the HM. Particular attention is paid to International Pupils to ensure they are able to contact their family at a suitable time.
5. During permitted hours, phones and headphones (unless authorised) should be out of sight and not used when walking around the campus in corridors and the Dining Hall – unless for emergency contact. This is applicable for staff and pupils. Phones may be used, at permitted times and for permitted year groups, in the V&A, the Library, the 6th form Centre and other agreed central spaces. Where there is an exceptional event, a decision on use will be communicated.
6. International pupils in the 3rd form may bring in a smart phone for travel reasons. This will be stored with the HM and may be permitted when needed.
7. Phones may be taken on away sports fixtures if leaving from the site and off-site visits but should not be visible or used at the venue unless authorised. It is expected phones are handed in. Trip leaders are responsible for overseeing.
8. If there are exceptional circumstances which require a pupil to have their phone, the HM will adjudicate and authorise as necessary in liaison with parents, if required.
9. Phones can be used from after College commitments on Saturday, and Sunday until hand-in times, unless otherwise specified. On Saturday evening phones should be handed in at lights-out for 3rd, 4th & 5th form.
10. Phones should not be visible at formal occasions. They must not be taken to Sunday evening Chapel.
11. There will be a scale of sanctions for misuse of mobile phones, including possessing an unauthorised additional device, overseen by the Head of Pupil Standards and Assistant Head (Pupils)
12. This policy will be reviewed when necessary and is encompassed within the Filtering and Monitoring Policy.

APPENDIX 2

Remote Learning Guidance

Please refer to [Providing Remote Education: Guidance for Schools](#) for further guidance. This guidance covers:

- when remote education should be used
- expectations for high-quality remote provision
- provision for pupils with SEND
- delivering remote education safely
- attendance considerations.

Further details are also included in '[Safeguarding and Remote Education](#)'. This includes information on:

- safeguarding children during remote learning
- expectations for staff behaviour online
- reporting safeguarding concerns
- safe use of live lessons and recorded lessons
- online safety
- pastoral support
- data protection and UK GDPR considerations.

During the Covid pandemic, teaching remote lessons became the norm. Despite returning to in-school, face to face teaching, we recognise that there may be occasions when students need to access lessons remotely (e.g. long-term illness) or in some circumstances one to one online teaching and tutoring occurs. The following guidance is to ensure that students are safeguarded, and staff are protected.

Technology

- The College policy is for Microsoft Teams to be used for all remote video conferencing. Microsoft Teams has been selected due to many considerations such as being able to use College email accounts (see later), the safeguarding of personal data, privacy questions and policies and terms of service. By deciding to use another means of communication, the relevant checks and safeguarding measures may not have been put into place.
- Avoid changing platforms if communication is disrupted by technical difficulties; reschedule the session instead.
- The usual safeguarding and AUP information applies: do not post or 'broadcast' anything which will bring you or the College into disrepute.
- Use only College provided equipment and do not use personal devices. If circumstances arise which necessitate you using a personal device (such as your College device breaking), you must inform the DSL and seek support from ICT.

Reporting

- Any safeguarding incidents / concerns should be reported to the DSL as soon as possible so that advice and support can be given. The DSL will log any such occurrences as a self-report.
- If there are issues over student behaviour during a video conferencing lesson, this should be reported to the Second Master and the Deputy Head (Academic)

One to One Video conferencing

1. When conducting a one-to-one video conference (via Teams) with a student it is important that you have checked the following:
 - a. You have invited another member of staff to a video conference you are conducting with a student/s. This may be the student's HM; tutor or DSL on duty during holiday periods. It is the invite (visibility of the meeting occurring) that is important here not their attendance in the video conference.
 - b. You have invited students and staff using their College email address.
 - c. Your background is free of unwanted imagery and personal affects. It is best practice to blur your background.
 - d. You are dressed appropriately.
 - e. Your language and tone must be professional and appropriate at all times.
 - f. Consider recording the session in order to protect you and the student/s.
2. Situations to avoid online and which may blur communication boundaries between you and the student are:

• A casual and intimate atmosphere	• Nicknames vs preferred Isams names
• Intimate locations	• Private conversations
• Casual and inappropriate dress	• Observational comments about home or family
	• Oversharing personal details
3. Doing the following is a breach of the College AUP and disciplinary action will be taken:
 - Taking photos or screen shots of students
 - Derogatory remarks
 - Being under the influence of alcohol or drugs whilst conducting a video conference call

Video Conference Call for remote learners

1. As a rule of thumb, if pupils are absent through illness, they should prioritise getting better. If they are too ill to attend school, they should not be accessing lessons on Teams.
2. In cases where the pupil is absent but is perfectly able to concentrate or is worried about getting behind (e.g. recovery from a broken limb), it is up to the teacher whether it is beneficial for that pupil to attend lessons via Teams. For example: if material is being explicitly taught, that would be a good lesson to attend virtually.
3. In these exceptional circumstances, Housemasters/mistresses will inform teachers when a student is in a situation where they would benefit from attending lessons virtually. Arrangements should be made in liaison with both HM and tutor.
4. Students should be invited to timetabled lessons via Microsoft Teams either by 'Schedule a meeting' or clicking the 'Meet now' button at the start of a lesson.
5. There is no requirement for you to record the lesson.
6. Keep a record of whether or not the student attends the lesson.
7. Ensure the student is able to view any shared content, e.g. PowerPoint, by sharing your screen.

Guidance for students and parents

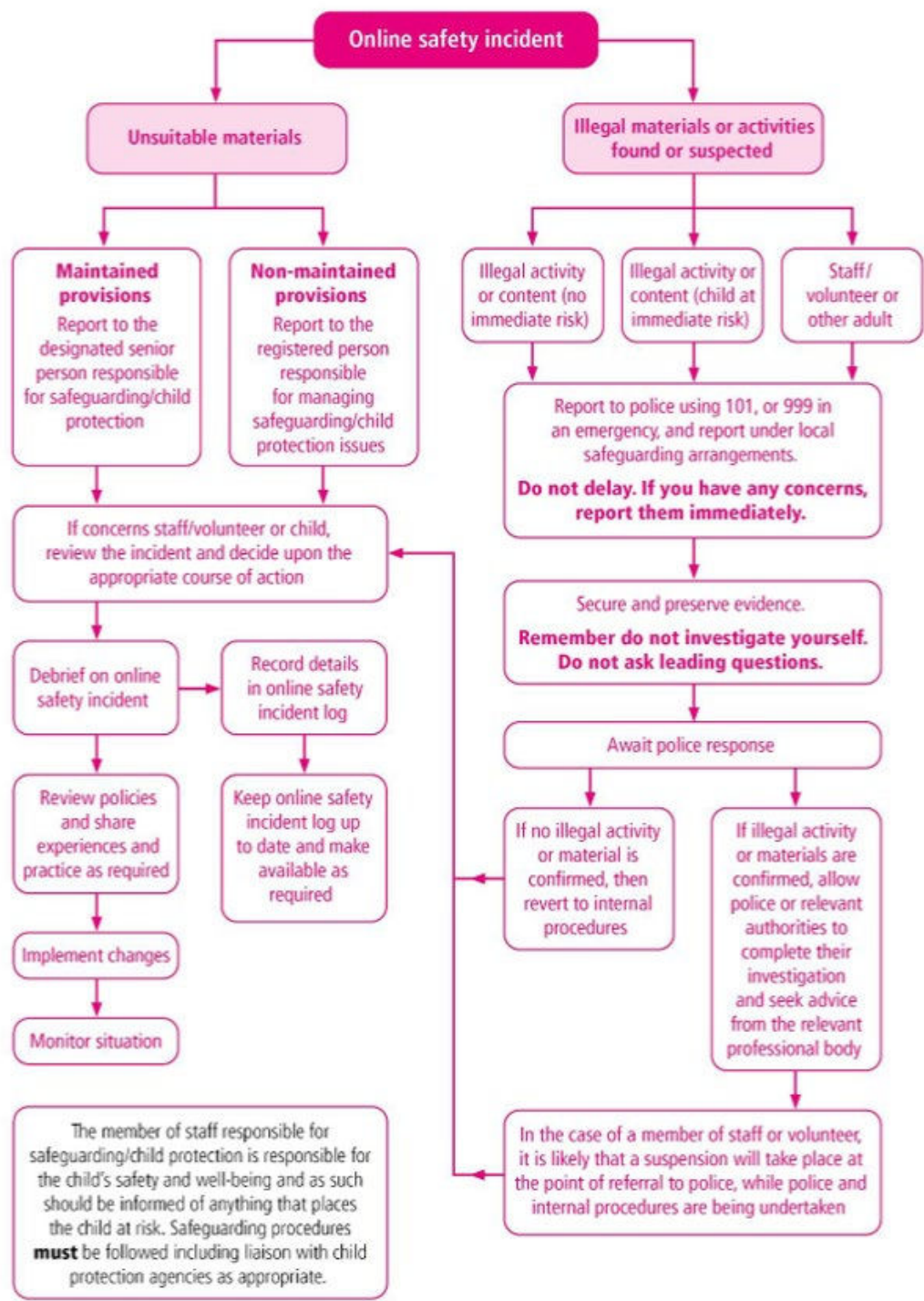
Whilst the above guidance is relevant to parents, carers and students, please note the following points:

1. When students are participating in a video conference or accessing lessons online, they should be in an environment which where possible is public and free from distractions.
2. Students should be dressed appropriately, adhering to standard classroom expectations.
3. Students should not record the lesson/video conference. Students should not share the video of the lesson/video conference with anyone without having received the express permission from the member of staff taking the lesson/conducting the video conference. Any breach will invoke a disciplinary response in line with the College AUP.

Appendix 3:

Online Safety Incident Flowchart

The following procedure will be followed if there is an incident of online safety (and in line with the child-on-child abuse, investigations and behavioural policies)



(Taken from https://hwb.gov.wales/api/storage/166ee994-c695-4ec2-af6c-a85bab5e9d11/Supporting%20document%2010_%20Online%20safety%20incident%20response%20flowcharts.pdf)

Appendix 4

Actions to be taken following an incident.

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures, however the grid below has been put together to help senior colleagues with decision making. It is not meant to be a definitive list of actions, but more of a guide.

Student Incidents	Refer to HM	Refer to Assistant Head (Pupils) / Second Master	Refer to Safeguarding team	Refer to Police / CSC	Refer to external expert for advice	Inform parents/guardians	Consider removing device / restricting	Issue a warning (record on iSams)	Further sanction in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).	X	X	X	X		X	X		X
Attempting to access or accessing the College network, using another user's account (staff or learner) or allowing others to access College network by sharing username and passwords	X	X	X			X	X		X
Corrupting or destroying the data of other users.	X	X				X	X		X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X			X
Unauthorised downloading or uploading of files or use of file sharing.	X	X				X			X

Using proxy sites or other means to subvert the College's filtering system.	X		X			X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X	X	X	X			X
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X	X		X		X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X				X		X	X
Unauthorised use of digital devices (including taking images)	X	X	X			X		X	X
Actions which could bring the School into disrepute or breach the integrity or the ethos of the School.	X	X	X			X		X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X	X	X	X	X	X	X

Responding to Staff Actions

Incidents	Refer to line manager	Refer to Head/ DSL	Refer to LADO	Refer to Police	Refer to LA / Technical Support Staff for action re filtering, etc.	Issue a warning	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	X	X	X	X			X
Deliberate actions to breach data protection or network security rules.	X	X	X		X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware. or software	X	X		X	X		X
Using proxy sites or other means to subvert the College's filtering system.	X	X			X	X	
Unauthorised downloading or uploading of files or file sharing	X	X				X	
Breaching copyright or licensing regulations.	X	X				X	
Allowing others to access School network by sharing username and passwords or attempting to access or accessing the College network, using another person's account.	X	X			X		X
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X	X
Using personal e-mail/social networking/messaging to carry out digital communications with learners and parents/guardians	X	X	X			X	X

Inappropriate personal use of the digital technologies e.g., social media / personal e-mail	X	X				X	X
Careless use of personal data, e.g., displaying, holding or transferring data in an insecure manner	X					X	
Actions which could compromise the staff member's professional standing	X	X	X			X	X
Actions which could bring the School into disrepute or breach the integrity or the ethos of the School.	X	X				X	X
Failing to report incidents whether caused by deliberate or accidental actions	X	X				X	X
Continued infringements of the above, following previous warnings or sanctions.	X	X	X				X

Appendix 5

Useful resources and tools for schools

UK Safer Internet Centre

- Safer Internet Centre – <https://www.saferinternet.org.uk/>
- Southwest Grid for Learning - <https://swgfl.org.uk/products-services/online-safety/>
- Childnet – <http://www.childnet-int.org/>
- Professionals Online Safety Helpline - <http://www.saferinternet.org.uk/about/helpline>
- Revenge Porn Helpline - <https://revengepornhelpline.org.uk/>
- Internet Watch Foundation - <https://www.iwf.org.uk/>
- Report Harmful Content - <https://reportharmfulcontent.com/>
- Harmful Sexual Support Service

CEOP

- CEOP - <http://ceop.police.uk/>
- ThinkUKnow - <https://www.thinkuknow.co.uk/>

Others

- LGfL – Online Safety Resources
- Kent – Online Safety Resources page
- INSAFE/Better Internet for Kids - <https://www.betterinternetforkids.eu/>
- UK Council for Internet Safety (UKCIS) - <https://www.gov.uk/government/organisations/uk-council-for-internet-safety>

Tools for Schools / other organisations

- Online Safety BOOST – <https://boost.swgfl.org.uk/>
- 360 Degree Safe – Online Safety self-review tool – <https://360safe.org.uk/>
- 360Data – online data protection self-review tool: www.360data.org.uk
- SWGfL Test filtering - <http://testfiltering.com/>
- UKCIS Digital Resilience Framework - <https://www.gov.uk/government/publications/digital-resilience-framework>
- SWGfL 360 Groups – online safety self-review tool for organisations working with children
- SWGfL 360 Early Years - online safety self-review tool for early years organisations

Social Networking

- Digizen – Social Networking
- UKSIC - Safety Features on Social Networks
- Children’s Commissioner, TES and Schillings – Young peoples’ rights on social media

Curriculum

- SWGfL Evolve - <https://projectevolve.co.uk>
- UKCCIS – Education for a connected world framework
- Department for Education: Teaching Online Safety in Schools
- Teach Today – www.teachtoday.eu/
- Insafe - Education Resources

Data Protection

- 360data - free questionnaire and data protection self-review tool

Wellington College online safety and mobile phone policy

- ICO Guides for Organisations
- IRMS - Records Management Toolkit for Schools
- ICO Guidance on taking photos in Schools

Infrastructure/Technical Support/Cyber-security

- UKSIC – Appropriate Filtering and Monitoring
- SWGfL Safety & Security Resources
- Somerset - Questions for Technical Support
- SWGfL - Cyber Security in Schools.
- NCA – Guide to the Computer Misuse Act
- NEN – Advice and Guidance Notes

Wellington College online safety and mobile phone policy

Appendix 6

Responding to AI generated child sexual abuse material

In June 2025, the IWF and CEOP Education (National Crime Agency) issued updated guidance to help schools respond to AI-generated child sexual abuse material (AI-CSAM).⁸

The guidance states clearly that:

- AI-generated images (e.g. face-swaps, nudification) are clearly defined as illegal pseudo-images
- Intent doesn't matter—even "fake" images are criminal

Guiding principles of dealing with AI-CSAM:

- Treat AI-generated CSAM the same as traditional CSAM
- Don't delete images – preserve the devices and evidence
- Inform the DSL immediately via the usual pathways
- The DSL will report to the incident to the police (calling 101 or 999 if there is immediate danger) as the primary pathway, with additional reports to CEOP or IWF as appropriate
- Use Childline's Report Remove for pupil-led takedowns (www.childline.org.uk/remove)
- The College will educate all students on the legal risks of creating or sharing AI-generated content

Emerging AI wearables and other AI-enabled recording devices may create additional safeguarding risks, including covert recording, live transcription, image capture, manipulation of content and the misuse of children's images or voice data. Staff should remain alert to these risks and treat any concern involving AI wearables in line with the College's safeguarding procedures, online safety policy and child-on-child abuse policy. Further guidance is available in the National Crime Agency / CEOP and Internet Watch Foundation guidance on AI-generated child sexual abuse material.

⁸ iwf.org.uk/media/ceel0u4z/ai-guidance-england-final.pdf

Responding to an incident



Any incident involving AI-CSAM should be treated with the same level of care, urgency and safeguarding response as any other incidence involving child sexual abuse material.

1. **Report it** to your DSL or equivalent.
2. **Follow the child protection and safeguarding policies** and procedures in your setting.
3. **Do not share, download or save the content** – even for reporting purposes. The decision to view any imagery should be based on the professional judgement of the DSL (or equivalent). The DSL should never copy, print, share, store or save them; this is illegal. For further information, please see UK Government's Guidance 'Sharing nudes and semi-nudes: How to respond to an incident'
4. **Encourage the young person not to delete anything** that could be used as evidence, such as messages, images, videos, usernames and URL links.
5. **Report it to the site, app or network** hosting it.
6. **Report it to the Police.** Call 101, or 999 if you believe the child or young person is in immediate danger.
7. **Consider wellbeing support.** As with any form of CSA, victims may need support to manage the emotional and psychological impact. Make victims of AI-CSAM aware of support in your setting and locally.

For further guidance on responding to incidents and reporting to statutory services, (including the police) visit: [sharing nudes and semi-nudes: advice for education settings working with children and young people.](#)

Children and young people can use the [Report Remove](#) tool from the IWF and Childline to report AI-CSAM that has been shared or might be shared online.

If a child or young person is in immediate danger report to the police by calling 999.