WELLINGTON
COLLEGE
PREP

Academic Year 2025 - 2026

Document Control	
Title of Policy:	**Online Safety Policy**
Policy / Procedure Owner:	Jessica Goves
Date Last Reviewed:	1st September 2025
Ratified by Governors:	3rd October 2025

Background and Rationale

Safeguarding young people at Wellington College Prep is taken very seriously. In the Wellington College Prep 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 Prep 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 Prep.

Keeping Children Safe in Education (2025) defines safeguarding as "protecting children from maltreatment; 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 Prep 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 Headteacher and Governors to the Senior 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 2025):

Content: being exposed to illegal, inappropriate or harmful content, or 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, sharing other explicit images and online bullying; and
Commerce - risks such as online gambling, inappropriate advertising, phishing[1] and or financial scams.

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

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:

- Behaviour policy
- Child-on-child abuse policy
- Safeguarding policy
- Acceptable Use Policy (AUP)
- Use of AI policy
- Filtering and Monitoring policy
- Social media 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 College Prep 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' (2025)
- 'Working together to Safeguard Children' (2018, updated December 2023)
- '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 (June 2025)

- The Online Safety Act (July 2025)

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 details on responding to AI-generated 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 children (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 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:

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

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

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

- Staff meetings and the All Staff Team.
-
- Governors' meeting / subcommittee meeting (Pastoral and Safeguarding subcommittee)
- Safeguarding newsletters for parents and staff
- School website

The policy will be reviewed annually by the Governors alongside the Safeguarding policy. The School 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 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 College Prep 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 online 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 and anti-bullying 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 2025[3] (page 38).

Roles and Responsibilities

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

The Headteacher and SLT

- The Headteacher 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

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

Deputy Head Pastoral, Deputy Head Safeguarding and the Head of Digital Learning & Strategy.

- The Headteacher and the SLT 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 Headteacher and the SLT 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 Online Safety team 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 School ethos, an undefended and reflective approach will be taken.
- Should a member of staff need any support following an online safety incident, the SLT will ensure that appropriate support be given to that individual and confidential counselling offered if needed.

Leadership of Online Safety

The Deputy Head Safeguarding (DSL) has overall responsibility for online safety within the school. The DSL will liaise closely with the Deputy Head Pastoral, Head of Digital learning and Strategy and the Head of LFL who will advise on the pastoral aspects of online safety and the education of online safety within the School (through the LFL+ programme; assembly/tutorial programme and computing lessons). They will meet at least twice termly with the Director of IT Development and Services 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 DSL 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 policy (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.
- Record online safety incidents and actions taken, in accordance with Wellington College Prep 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.
- Liaise with the local authority and other local and national bodies as appropriate.
- To lead the Online Safety Team (which includes the Head of Digital Strategy and Learning; member of Wellington College IT Services and two DDSL's), who will work together to

[4] https://www.headstartkernow.org.uk/for-prof/digital-resilience/

improve online safety awareness amongst the school community 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;
    - 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 Director of Safeguarding informed of any serious incidents and concerns and take responsibility for implementing actions as appropriate liaising with Senior Deputy Head over disciplinary decisions.
- Work with the Director of IT Services and technical support staff, to ensure that appropriate filtering and monitoring is in place.
- 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 Wellington 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 2025).
- 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.
- Ensure that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches.
- 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 Prep'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 SLT team and other agencies, where appropriate.

The DSL 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 Deputy Head Safeguarding has regular meetings with the Safeguarding team in order to keep the safeguarding team abreast of online safety issues both nationally and within the School. The DSL also attends and reports to Safeguarding team meetings at Wellington College.

The Director of IT Development and Services/ IT Staff(Wellington College Prep)

The Director of IT Development and Services, Wellington College IT Services Department and the College IT services department(Wellington College Prep) 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 policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.
- That they keep up to date with online safety technical information in order to effectively carry out their online 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 Deputy Head Safeguarding for investigation / action / sanction.
- That monitoring software / systems are implemented and updated as agreed in school policies.
- That Wellington College IT Services liaise at least fortnightly with Deputy Head Safeguarding reporting any concerns. A fortnightly meeting is scheduled between the Deputy Head Safeguarding and Director of IT and Services.

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
- They have read, understood and signed the school 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 Deputy Head Pastoral or Deputy Head Safeguarding for investigation / action / sanction (any decision of which will be made in conjunction with the Senior Deputy Head)
- 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
- Students understand and follow the school online safety and Acceptable Use Policy
- Students from Year 3 and up, have a good understanding of research skills and how to conduct good internet searches. They monitor ICT activity in lessons, extra curricular and extended school activities.
- Students' use of AI in their learning is only carried out with adult supervision and any AI platforms that are used must have the permission of the Director of IT and the Head of Digital Strategy and Learning, as detailed in the Use of AI Policy.
- They are aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices.
- 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
- 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 Safeguarding newsletters, letters home, the School website and access to National Online Safety platform (Wellington College Prep is a member of the National College).

Parents also need to be aware that if their children (this applies to boarders only) are supplied with a 3G/4G/5G mobile device they will be able to access the internet independently of the School system and therefore the School 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 School 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 School provides over the course of the academic year
- Supporting the School actions where an online 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

Access to electronic devices

- In Nursery to Year 4 the school will provide computers and personal devices for use during lessons. In Years 3-and 4 , these are named devices. Pupils and staff are responsible for looking after the school devices and ensuring that they are returned and charging properly.
- Pupils in Year 5 purchase a Microsoft Surface device for use in lessons until the end of Year 8, or when they leave the school. These devices are owned by the parents but managed by the school. It is the pupils' responsibility to ensure that it is in school each day which is charged, regularly updated and in working order.
- All pupil devices are school managed. No other devices are allowed.
- Pupils are not allowed to carry mobile phones during school hours. Boarders are allowed limited access to mobile *phones* and internet use. (Please see boarder's handbook for further details).
- Smart watches are not allowed during the school day.

Internet usage

- All pupils have access to a Microsoft 365 account for use across the curriculum. This is primarily used by Years 4-8. This is managed and filtered by Wellington IT Services.
- The platform, Seesaw, is used from Early Years to Year 3 with parents having access to their child's online journal.
- Good use of the internet for safety and wellbeing will be taught both during LFL+, Enrichment and Digital Learning lessons and embedded within all academic lessons where the internet is used.
- Internet access will be planned to enrich and extend learning activities. When using the internet they will be given clear objectives for its use.
- Pupils must ask permission before accessing the internet and have a clear idea of why they are using it.
- The internet must only be used by pupils for academic work. Educational games and apps may only be used with permission from a teacher.
- If staff or pupils discover unsuitable sites, the URL, time and content must be reported to their teacher, Deputy Head Safeguarding and IT Services who will investigate and take appropriate action
- School will ensure that the use of internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.
- Pupils will be taught what internet use is acceptable and what is not. Staff will guide pupils in online activities that will support learning outcomes planned for the pupils' age and maturity.

- Pupils will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation.

Use of AI

- To ensure appropriate use and compliance with data protection and safeguarding standards, pupils must be 13 years or older to independently access and use Generative AI tools. Pupils under the age of 13 may only use AI tools with explicit permission from the Director of IT and Head of Digital Learning at WCP, An adult must be present during use to ensure that the necessary checks and safeguards are in place.
-

Email & Online Collaboration

- Pupils may only use approved email accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive messages.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission.
- Pupils must not access others pupil's accounts or files.
- Pupils must be responsible for their own behaviour on the internet, just as they are anywhere else in the school. This includes the materials they choose to access, and the language they use.
- Pupils must not deliberately seek out offensive materials. Should any pupils encounter any such material accidentally, they are expected to report it immediately to a teacher, so that the school can block further access to the site.
- Pupils are expected not to use any rude or offensive language in their communications and contact only people they know or those the teacher has approved. They will be taught the rules of etiquette for email and will be expected to follow them.
- The internet should not be used by pupils during the school day for any social networking. (Please refer to the Mobile Phone and portable Device policy for details on boarders outside the school day.)
- Pupils are advised never to give out personal details of any kind that may identify them or their location.
- Pupils are advised on security and encouraged to set passwords.

Prep

- Staff are at liberty to set prep to be completed at school/home that requires a computer or device. This is largely through the Microsoft Teams platform.
- Pupils are encouraged to work on school recommended apps and sites to a reasonable degree in their own time away from school to practise their skills in various subjects.
- Wednesday afternoon Boarders' prep in school is regarded as 'Home Prep' and computers may be used by all those who attend. However, duty staff must ensure that they are fully aware of what the children are using their computer for at this time and be very mobile around the classroom.

Times when the use of devices and the internet are prohibited

- **Registration and Tutor Time**
    - Personal computer and device use at this time should only be for charging devices; to check emails and quick retrieval practice e.g. Spelling Shed, Mathletics. This will be closely monitored by the tutor.

- **Outside Curriculum time**
    - Pupils should not be using computers or devices in the library, art room, form rooms during any break time (unless directly supervised by an adult) or at pick-up.

Boarders and outside school hours advice

- Pupils are advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Pupils are encouraged to invite known friends only and deny access to others.
- Pupils and parents are made aware that some social networks are not appropriate for children of primary school age and the legal age to hold accounts on many such as YouTube (18 years old) or Instagram (13 years old) are older than primary school age children.

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:

- Year 3-8 pupils will sign a pupil friendly Acceptable Use Policy (located in their planners) at the start of each academic year and will be reminded by tutors that internet use will be monitored. Years 1 & 2 pupils will have the AUP explained to them in their lessons and a pupil friendly poster featuring the AUP will be placed in classrooms.
- A planned online safety programme is provided as part of the LFL+ programme, Digital Learning and academic lessons. In addition to this, key online safety messages (based on resources from Education for a Connected World framework) will be reinforced to each year group through assemblies led by the DSL. The content of lessons and talks will be regularly reviewed so that they are up to date and relevant.
- The DSL will highlight the issue of sexting to Year 7 & 8 pupils in early Michaelmas term through assemblies 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).
- Boarders using mobile phones, outside school hours will be given strict rules about their use.
- 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
- Rules for internet access including aspects of the AUP will be posted in all classrooms.
- Pupils can use the 'Feeling Concerned' tab on their login screen to report anything which is worrying them.

Outline:

Year Group	Where learning occurs	What is taught & discussed
In **Early Years** the internet is used to access age-appropriate software and apps. These are set up and closely monitored by staff when in use.		
Years 1&2	Curriculum lessons Digital Learning LFL+	Safe passwords Information that is safe/unsafe to share Ways to get help Gaming and using chat rooms- what is age appropriate for PP children Introduction to safe sites / using search engines
Years 3&4	Curriculum lessons Digital Learning LFL+	Safe passwords, appropriate sharing of information Information that is safe/unsafe to share Ways to get help Respect and kindness online - cyberbullying Using search engines What games and chat rooms to use and when are they age appropriate. Digital resilience.
Year 5&6	Curriculum lessons Digital Learning Enrichment LFL+	Safe passwords, appropriate sharing of information Social media and chat rooms pros and cons Ways to get help Respect and kindness online - cyberbullying Online gaming, age-appropriateness Phishing, scams, fake information. Digital resilience.
Year 7	Curriculum lessons Digital Learning Enrichment LFL+	Safe passwords, appropriate sharing of information Social media and chat rooms pros and cons – mental health and wellbeing Respect and kindness online - cyberbullying Online gaming Phishing, scams, fake information Developing a positive online footprint

		Digital resilience.
Year 8	Curriculum lessons Digital Learning Enrichment LFL+	Safe passwords, appropriate sharing of information Safe use of social media – mental health and wellbeing Online gaming Respect and kindness online - cyberbullying Phishing, scams, fake information Sexting, sexual harassment Positive body image – Pornography Digital resilience.

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:

- Termly safeguarding newsletter
- Access to the National Online Safety training platform
- Parent talks

Parents' attention will be drawn to their child's Acceptable Use Agreement in the child's planner and the following policies in newsletters, communication home and the school website:

- Online safety Policy;
- AUP of ICT Policy;
- Child-on Child Abuse Policy (which includes antibullying and sexual misconduct);
- Mobile Phone and Portable Device;
- Use of AI Policy.

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 to have read the School online safety policy and the Use of AI policy;
- all staff and their families (who have access to the school network) to 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 Online Safety training platform in order to keep abreast of up-to-date information on online safety issues;

- the Deputy Head Safeguarding will provide advice / guidance / training as required to individuals as required e.g. through safeguarding notices in staff meetings safeguarding newsletters and National College platform;
- staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

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 platform courses/guides/webinars.

Incident Management Procedures

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

- there are clear reporting routes which are understood and followed by all members of the School community which are consistent with the School safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies;
- •all members of the School 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 School safeguarding procedures, this may include:
  - o non-consensual images;
  - o self-generated images;
  - o Terrorism/extremism;
  - o Hate crime/ Abuse;
- o Fraud and extortion;
- o Harassment/stalking;
- o Child Sexual Abuse Material (CSAM);
- o Child Sexual Exploitation Grooming;
- o Extreme Pornography;
- o Sale of illegal materials/substances;
- o Cyber or hacking offences under the Computer Misuse Act;

- o Copyright theft or piracy;
  • any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, 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 Team 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, Behaviour and safeguarding risk management policies.

Technical – infrastructure / equipment, filtering and monitoring

Wellington College will be responsible for ensuring that Wellington College Prep infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. Wellington 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).

It 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 DSL and Director of IT Development and Services. These audits and any action points will be shared with the SLT;
- 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 Development and Services and will be reviewed, at least annually, by the Head of Digital Strategy and 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;
- Wellington College Prep has provided enhanced user-level filtering through the use of the Lightspeed & Palo Alto filtering programmes. 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 Headteacher or the DSL;
- requests from staff for sites to be removed from the filtered list will be considered by the DSL and the Head of Digital Strategy and Learning;
- 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 Head of Year and permission sought through the DSL;
- there are occasions when staff may need to email pupils and vice versa at Wellington College Prep. The Director of IT Services and Development will randomly sample staff to student emails (this should include all staff, not just teaching staff) and send a report to the DSL monthly:
    - 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 their findings to be sent to the 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 School 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, work stations, hand held 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 DSL 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 WC IT Services 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 Deputy Head Safeguarding (DSL).
- 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 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 Safeguarding (DSL).
- 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 Safeguarding (DSL).
- **All members of staff working in EYFS will not use or carry personal mobile phones or other personal electronic devices which have imaging and sharing capabilities while working.** Staff may use their personal device during break and lunchtimes in the staff room or personal office only. Designated school iPads and/or surface, which are managed by IT systems, are used to take photos and record information for See Saw and the children's Learning Journals.

- 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 School's Term and Conditions clarifies what is permissible and parents are required to opt out of the sharing of such images when signing the Wellington College Prep 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).
- 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 ICT Acceptable Use Policy. In the context of online 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 Senior Deputy Head. 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 tutor or Pastoral Lead in the first instance. The email should be printed and saved before any further action is taken by the Senior Deputy Head.
- Any digital communication between staff and students (emails) or parents (emails and What's app groups) 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 school)social media sites will be uploaded by Head of Marketing and content is monitored by the Senior Deputy Head. They are also subject to the disciplinary procedures of the School and the Facebook and X (formally 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 Wellington College Prep Safeguarding policy details the school's 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 law[5]
- 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 UK[6]
- 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 colleagues, 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
- 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 Deputy Head Safeguarding (DSL) or the Senior Deputy Head. All staff are reminded that there is a clear School Whistleblowing policy (accessed on All Staff Team) which they should refer to.

Reviewed by JCG Sept 2024 to include KCSIE 2024 changes

Reviewed by JCG Sept 2025 to include KCSIE 2025 changes

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

[6] https://www.cps.gov.uk/legal-guidance/obscene-publications