The Study Prep

WIMBLEDON

Name of Policy	E Safety Policy
Reviewed by	Head of Computing
HMT Member	Deputy Heads/DSLs
Date of review	January 2024
Date of next review	February 2025

The Study Prep
WIMBLEDON

E Safety Policy

Introduction

The Study Preparatory School recognises that technology has transformed the lives of young people today, providing them with enormous opportunities to learn, communicate, research and play. However, with the increase of online activity and access to devices there is now greater exposure to potential risks and challenges. The school has a duty to provide a safe environment for learning and teaching for both staff and pupils.

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

- **Conduct:** personal online behaviour that increases the likelihood of, or causes harm. For example: sending and receiving explicit images or messages.
- **Content**: being exposed to illegal, inappropriate or harmful material; for example racist or radical and extremist views.
- **Contact**: being subjected to harmful online interaction with other users; for example cyberbullying or online grooming
- **Commercial exploitation**: for example young people can be unaware of hidden costs and advertising in apps, games and websites

An important part of the School's role is to teach pupils and staff how to stay safe in the changing online environment and how to avoid making themselves vulnerable to a range of risks including, but not limited to the risk of identity theft, cyber bullying, harassment, grooming, stalking, abuse and radicalisation as well as how to manage their digital footprint in such a way as to avoid future embarrassment. All staff attend an annual online safety briefing update and receive regular updates via staff meetings, briefings, email and training sessions. The School raises awareness of online safety issues on Safer Internet Day, through whole school training, lessons and participation in workshops. This policy should be read in conjunction with the Digital Camera and Mobile Phone Policy as well as the Acceptable Use Agreements.

All users need to be aware, in an age-appropriate way, of the range of risks associated with the use of these internet technologies. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs, forums and chat rooms;
- Mobile internet devices such as smart phones and tablets;
- Social networking sites;
- Music / video downloads;
- Gaming sites and online communities formed via games consoles;

- Instant messaging technology via SMS or social media sites;
- Video calls;
- Podcasting and mobile applications;
- Virtual and augmented reality technology; and
- Artificial intelligence.

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

Aim

Online safety is paramount to safeguarding and the school has a duty to ensure that all pupils and staff are well informed and kept up to date with strategies to prevent, manage and respond to risk online.

The aim of this policy is to promote responsible behaviour with regard to online activities, protect the interests and safety of the whole school community and foster the critical thinking skills necessary to enable pupils and staff to remain safe online.

Scope

This policy applies to the whole community at The Study including teachers, governors, supply teachers, support staff, contractors, visitors, catering staff, parents/carers and all children including EYFS. It applies to anyone who has access to and are users of the school IT systems. In this policy:

- “staff” includes teaching and non-teaching staff, governors, and volunteers;
- “parents” includes pupils' carers and guardians; and
- “visitors” includes anyone else who comes to the school.

Both this policy, and the Acceptable Use policies, cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

The policy provides guidance to online safety behaviours such as cyberbullying both in school and if necessary incidents that happen outside school.

Roles and Responsibilities

All staff, governors and visitors have responsibilities under the safeguarding policy to protect children from abuse and make appropriate referrals. The following roles and responsibilities must be read in in line with the Safeguarding and Child Protection Policy.

The Governing Body

The Governing Body has overall leadership responsibility for safeguarding as outlined in the Safeguarding and Child Protection Policy. The Governing Body of the school is responsible for the approval of this policy and for reviewing its effectiveness at least annually.

The Governing Body will ensure that all staff undergo safeguarding and child protection training, both at induction and with updates at regular intervals, to ensure that:

- all staff, in particular the Online safety Coordinator, DSLs and HMT are adequately trained about online safety;

- all staff are aware of the expectations, applicable roles and responsibilities in relation to filtering and monitoring and how to raise to escalate concerns when identified;
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

Head and HMT

The Head is responsible for the safety of the members of the school community and this includes responsibility for online safety. Together with HMT, they are responsible for procuring appropriate filtering and monitoring systems, documenting decisions on what is blocked or allowed and why, reviewing the effectiveness of the filtering and monitoring provisions, overseeing reports and ensuring staff are appropriately trained.

DSLs

The DSLs takes the lead responsibility for Safeguarding and Child protection at The Study Prep, this includes a responsibility for online safety as well as the school's filtering and monitoring system.

The DSLs will ensure that this policy is upheld at all times, working with the Head, the Head of Computing and the IT Manager IT staff to achieve this. As such, in line with the Safeguarding and Child Protection policy, the DSLs will take appropriate action if in receipt of a report that engages that policy relating to activity that has taken place online.

The DSLs will work closely with the Online Safety Co-ordinator and the school's IT service providers to ensure that the school's requirements for filtering and monitoring are met and enforced. The DSLs will review filtering and monitoring reports and ensure that termly checks are properly made of the system.

DSL: Sarah Lee (Deputy Head Wilberforce House) and Chris Baalham (Deputy Head Spencer House)
DDSL: Sharon Maher (Head)
DDSL: Melissa Peachey (SENCO)
DDSL: Karen Lee (Head of EYFS)

All have been trained in e-safety issues which may arise as a result from misuse of the internet, such as:

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate contact on-line with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.

Should the School discover that a pupil is at risk as a consequence of online activity, it will seek assistance from the appropriate authorities such as the Child Exploitation and Online Protection Unit (CEOP), the police and/or Merton Council.

Technical Staff

The School's IT Manager is responsible for ensuring that the IT infrastructure is not open to misuse or malicious attack and ensure that users may only access the networks through an enforced password protection policy. He/she will also ensure that appropriate monitoring and filtering systems are maintained and set up so that any potential safeguarding issues are emailed to the safeguarding team as and when they happen.

E Safety Coordinator

The School's computing specialist ensures online safety is embedded in the teaching and learning of the subject. They will keep up to date on current online safety issues and guidance issued by relevant organisations, including the Department for Education (including KCSIE), ISI, the CEOP (Child Exploitation and Online Protection), Childnet

International and the Local Safeguarding Children Procedures. The Head of Computing will share any disclosure, report or suspicion of improper use of school IT or any issues with the school's filtering and monitoring system to the DSL.

They will make necessary updates to the pupil Acceptable Use Agreements which are sent out to parents and pupils to sign at the start of each school year. Staff receive regular training on online safety and that they are fully aware of this guidance and the associated policies. Parents are offered regular online safety guidance.

Teaching and Support Staff

Teaching staff should have an up to date awareness of online safety matters and of the current School E Safety Policy and practices. They should report any suspected misuse or problem to the DSLs/Deputy DSLs and/or the Head of Computing. Staff are not permitted to give their personal mobile phone numbers or email addresses to parents or pupils and should not communicate with them by text message, personal email or social media. Full details of these guidelines are set out in the Staff Code of Conduct. Staff should ensure that all digital communications with pupils/parents/carers/fellow staff are on a professional level and conducted on school systems.

Teaching staff should be aware that online safety issues are embedded in all aspects of the curriculum and other school activities and should ensure pupils understand and follow the Acceptable Use Agreement. All staff are required to sign and return the [IT Acceptable Use Policy] before accessing the school's systems. As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

All staff must read and understand this Online Safety Policy and enforce it in accordance with direction from the DSL, the Head and HMT.

Teaching staff should monitor and supervise online activity in lessons and extra-curricular activities and should be aware of online safety issues related to the use of digital devices. Pupils should be guided to sites checked as suitable for their use and if unsuitable material is found in Internet searches this should be reported immediately to the Head of Computing and/or IT Manager. Teaching staff should ensure that they have pre-viewed sites used in the classroom or set for homework purposes. Where internet research is set for a pupil, teachers should always recommend suitable websites and provide safe links.

Teaching staff need to be aware that certain groups of children may be more vulnerable to acts of cyberbullying, particularly children who experience difficulties at home, lack supportive adult role-models or have special educational needs/disabilities. These groups of children are likely to be more upset by disturbing online material and less likely to report incidents.

Pupil Conduct

Pupils are taught how to use technology safely, responsibly, respectfully and securely in accordance with the Pupil Computing Agreement which is shared with parents and signed annually. They are taught where to go for help and support when they have concerns about content, contact or conduct online. The School expects pupils to treat each other online with the same standards of consideration, respect and good manners as they would in the course of face-to-face contact both in and out of school. All pupils are encouraged to support each other and to report any concerns about the misuse of technology to a member of staff. The School will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Anti-bullying Policy. Only Year 6 pupils are permitted to bring a mobile phone into School and these must be clearly labelled and handed in at the start of the school day. Permitted use of cameras and mobile phones is detailed in the Digital Camera and Mobile Phone Policy and is explained to Prep School pupils as part of their PSHE lessons.

Parents and carers

Parents/carers are expected to read and discuss the pupil Acceptable Use Agreement with their daughter and sign at the start of each academic year. Parents and carers are invited to attend online safety training organised by the school and receive updates via school communication. Parents will be informed if their daughter is in breach of the agreement or if their daughter is involved in a cyberbullying related incident.

Filtering and Monitoring

In general:

The Study Preparatory aims to provide a safe environment to learn and work, including when online. Filtering and monitoring are important parts of the school's safeguarding arrangements and it is vital that all staff understand the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

Staff, pupils, parents and visitors should be aware that the school's filtering and monitoring systems apply to all users, all school owned devices and any device connected to the school's internet server. Deliberate access, or an attempt to access, prohibited or inappropriate content, or attempting to circumvent the filtering and monitoring systems will be dealt with under the Staff Code of Conduct or the Behaviour Policy, as appropriate.

The Online Safety Coordinator will check once per term that the filtering and monitoring system are operating effectively – these checks must be recorded along with any appropriate action. From time to time the Safeguarding and/or Online Safety governor, the DSL and Online Safety coordinator will review the filtering and monitoring system, looking at the records of the checks. Such a review should occur before the beginning of every new academic year, however such reviews should occur if:

- there is a major safeguarding incident;
- there is a change in working practices; or
- if any new technology is introduced.

The school's filtering system blocks internet access to harmful sites and inappropriate content. The filtering system will block access to child sexual abuse material, unlawful terrorist content, and adult content. If there is a good educational reason why a particular website, application, or form of content should not be blocked a pupil should contact the relevant member of teaching staff, who will then contact the Online Safety Coordinator and DSL for their consideration.

The school will monitor the activity of all users across all of the school's devices or any device connected to the school's internet server allowing individuals to be identified. In line with the school's Data Protection Policy and/or Privacy Notice/s, the DSLs receive an alert when an attempt to access inappropriate material has been made, should further investigation be required, a DSL will follow up with the IT Manager and will monitor the logs daily. Any incidents should be acted upon and recorded. If there is a safeguarding concern, this should be reported to the DSLs immediately. Teaching staff should notify the Online Safety Coordinator, their Head of Department and a DSL if they are teaching material which might generate unusual internet traffic activity.

Staff:

If any member of staff has any concern about the effectiveness of the filtering and monitoring system, they must report the matter to a DSL immediately in line with the Safeguarding and Child Protection Policy; particularly if they have received a disclosure of access to, or witnessed someone accessing, harmful or inappropriate content.[If any member of staff accidentally accesses prohibited or otherwise inappropriate content, they should proactively report the matter to a DSL.

While the filtering and monitoring system has been designed not to unreasonably impact on teaching and learning, no filtering and monitoring system can be 100% effective. Teaching staff should notify a DSL if they believe that appropriate teaching materials are being blocked.

Pupils:

Pupils must report any accidental access to materials of an inappropriate nature to the appropriate teacher. Deliberate access to any inappropriate materials by a pupil will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for school work / research purposes, pupils should inform the relevant teacher.

Education and training

Staff: awareness and training

As part of their induction, all new teaching staff receive information on online safety, including the school's expectations, applicable roles and responsibilities regarding filtering and monitoring. This will include training on this Online Safety Policy.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following the school's Online Safety procedures.

All staff receive regular information and training (at least annually) on online safety issues in the form of INSET training and internal meeting time, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. All supply staff [and contractors] receive information about Online Safety as part of their safeguarding briefing on arrival at school.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. When pupils use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

In accordance with the Safeguarding and Child Protection Policy, if there is a safeguarding concern a report must be made by staff as soon as possible if any incident relating to online safety occurs and be provided directly to a DSL.

Pupils: the teaching of online safety

Online safety guidance will be given to pupils on a regular basis. We continually look for new opportunities to promote online safety and regularly monitor and assess our pupils' understanding of it.

Online safety is fully embedded within our curriculum. The school provides a comprehensive age appropriate curriculum for online safety which enables pupils to become informed, safe and responsible. The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via PSHE / RSE, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their online safety responsibilities and to look after their own online safety. Pupils can report concerns to a DSL and/or any member of staff at the school.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Safeguarding and Anti Bullying Policies, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL, or any other member of staff they trust, as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

The curriculum is flexible and can respond to any immediate online safety issues and risks as they emerge.

It is necessary for pupils to develop skills of critical awareness, digital resilience and good online citizenship to enable them to use internet, mobile and digital technologies safely and responsibly. Pupils are taught to recognise the creative, collaborative, cultural, economic and educational opportunities provided by the internet, mobile and digital technologies. Curriculum work will also include areas such as:

- Understanding how to use the internet, mobile and digital technologies in a balanced and appropriate way to avoid negative impact on wellbeing, e.g. regulated screen time and diverse online activity
- Learning how to develop a positive online reputation and enhance future opportunities e.g. in relationships and employment
- Developing critical thinking skills and the confidence to challenge and question what they see and read in relation to online content e.g. recognising fake news and extremism, understanding commercial manipulation, maintaining an authentic sense of self that is resilient to online pressure, learning how easy it is to lie online (i.e. users may not be who they say they are and may have ulterior motives Understanding the dangers of giving out personal details online and the importance of maintaining maximum privacy online
  Thinking carefully before placing images online and considering their appropriateness and understanding the importance of gaining consent before posting photographs of others
- Understanding the permanency of all online postings and conversation.
  Understanding relevant legislation, including copyright, and the importance of respecting other people's information, reputation and images.
- Understanding the importance of online respect and what constitutes cyberbullying, how to avoid it, the impact it has and how to access help.
- How the law can help protect against online risks and abuse

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.

Staff are referred to the BYOD Policy, staff code of conduct and IT Acceptable Use Policy for further guidance on the use of non-school owned electronic devices for work purposes.

Staff are permitted to bring in personal devices for their own use. They may use such devices in the staffroom only during break-times and lunchtimes.

Staff are not permitted under any circumstances to use their personal devices when taking images, videos or other recording of any pupil nor to have any images, videos or other recording of any pupil on their personal devices. Please read this in conjunction with Safeguarding and Child Protection, Acceptable Use, Staff Code of Conduct and School Trips policies.

Pupils

If pupils bring in mobile devices (only for Year 6 for use during the journey to and from school), they should be handed to the School Secretary at the start of the day and collected as they leave school. These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.

Pupils are responsible for their conduct when using school issued or their own devices. Any misuse of devices by pupils will be dealt with under the School’s Behaviour Policy.

Online Communications

Staff

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer / [recent alumni (i.e. pupils over the age of 18 who have left the school within the past 12 months) or parents of recent alumni] using any personal email address or SMS / WhatsApp. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business. Personal telephone numbers, email addresses, or other contact details, may not be shared with pupils or parents / carers [and recent alumni]. Under no circumstances may staff contact a pupil or parent / carer [and recent alumni] using a personal telephone number, email address, or other messaging system nor should pupils, parents [and recent alumni / their parents / carers] be added as social network 'friends' or similar.

Staff must immediately report to a DSL / Head the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the Head/IT Manager.

Pupils

All pupils are issued with their own personal school email addresses for use on our network. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all school work] [assignments / research / projects. Pupils should be aware that email communications through the school network and school email addresses are monitored.

The school will ensure that there is appropriate and strong IT monitoring and virus software. Spam emails and certain attachments will be blocked automatically by the email system.

Pupils must not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and should immediately report such a communication, to a member of staff who should then refer it to a DSL.

Use of social media

Staff

When accessed from staff members' own devices / off school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school in accordance with the Staff Code of Conduct.

Any online communications, whether by email, social media, private messaging or other, must not:

- place a child or young person at risk of, or cause, harm;
- bring [name of school] into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;

    - using social media to bully another individual; or
    - posting links to or endorsing material which is discriminatory or offensive.
- otherwise breach the Staff Code of Conduct or Child Protection and Safeguarding Policy.

Pupils

The school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted must not be, or potentially be, inappropriate or offensive, or likely to cause embarrassment to an individual or others. The school takes misuse of technology by pupils vary seriously and incidents will be dealt with under the Behaviour, Safeguarding and Child Protection and Anti-Bullying policies as appropriate.

Data protection

Please refer to the Data Protection policy and the IT Acceptable Use Policy for further details as to the key responsibilities and obligations that arise when personal information, particularly that of children, is being processed by or on behalf of the school.

Staff and pupils are expected to save all data relating to their work to their school laptop or the Google Drive Account.

Staff devices should be encrypted if any data or passwords are stored on them. Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal memory sticks, but instead stored on an encrypted USB memory stick provided by the school.

Staff should also be particularly vigilant about scam / phishing emails (and similar) which could seriously compromise the school's IT security and/or put at risk sensitive personal data (and other information) held by the school. If in any doubt, do not open a suspicious email or attachment and notify the IT Manager in accordance with the Data Protection Policy and IT Acceptable Use Policy.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the IT Manager

Password security

Pupils and staff have individual school network logins, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper- and lower-case letters as well as numbers), which should be changed every 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff should inform and educate pupils 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 (personal) images on the internet (e.g. on social networking sites) and follow the School's policy on official social media posting.

Artificial Intelligence

The School does not permit the use of generative AI tools such as ChatGPT on school devices / systems. In particular, personal or confidential information should not be entered into generative AI tools. This technology stores and learns from data inputted and you should consider that any information entered into such tools is released to the internet.

Misuse

The School will not tolerate illegal activities or activities that are in breach of the policies referred to above. Where appropriate the school will report illegal activity to the police and/or the local safeguarding partnerships. If a member of staff discovers that a child or young person is at risk as a consequence of online activity they should report it to a DSL. The DSL then may seek assistance from the CEOP, the LADO, and/or its professional advisers as appropriate.

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Safeguarding and Child Protection and Behaviour policies.

Complaints

As with all issues of safety at the School if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the relevant teacher in the first instance, who will liaise with HMT and the Head and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of, or concerns around online safety will be recorded in accordance with the Safeguarding and Child Protection policy and reported to a DSL in accordance with the school's Safeguarding and Child Protection Policy.

Related Policies

- Digital Camera & Mobile Phone Policy
- Staff Code of Conduct
- Anti-Bullying Policy
- Safeguarding Policy
- Acceptable Use Agreements

Policy reviewed: January 2024