The Study Prep
WIMBLEDON

Name of Policy	E Safety Policy
ISI Regulation	3: Welfare, health and safety of pupils
Reviewed by	Head of Computing
HMT Member	Deputy Heads
Date of review	November 2022
Date of next review	November 2023

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 online safety briefing update at the start of the year 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.

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 Prep including teachers, governors, supply teachers, support staff, contractors, visitors, catering staff, parents/carers and all children including EYFS. It applies to anyone accessing school systems, network and internet using school technology and devices or personal devices.

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

DSL: Sarah Lee (Wilberforce House) and Chris Baalham (Spencer House)
DDSL: Helen Lowe(Interim Head)

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.

Their role is to lead a 'safeguarding' culture, ensuring that online safety is fully integrated within whole school safeguarding.

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 ICT 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 filters and safeguards are in place to filter and monitor inappropriate content 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 ensure that online safety incidents are reported to the Head who keeps a log of these. They will make necessary updates to the pupil Acceptable Use Agreements which are sent out to parents and pupils 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 Designated Safe Guarding Lead/Deputy DSL and/or the E Safety Coordinator. 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. 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 Computing Lead and/or ICT 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's Computing Agreement which is shared with their 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 Prep School 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.

Curriculum

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 PSHE Curriculum, Relationships and Health Curriculum are central in supporting the delivery of online safety education.

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

Reporting incidents, abuse and inappropriate material

There may be occasions in school when either a pupil or an adult receives an offensive, abusive or inappropriate message or accidentally accesses upsetting or abusive material. When such a situation occurs the pupil or adult must report the incident immediately to the first available member of staff, their class teacher or the E Safety coordinator. Where such an incident may lead to significant harm, safeguarding procedures should be followed. The school takes the reporting of such incidents seriously and where judged necessary, will refer details to social care or the police (CEOP).

Related Policies

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

Policy reviewed: February 2023