



WELLESLEY PREP SCHOOL

E-SAFETY POLICY

This policy applies to all parts of Wellesley Prep School including the Early Years Foundation Stage.

Updated: Sept 2023
Review Date: Sept 2024

INTRODUCTION

It is the duty of Wellesley Prep School to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are, therefore, taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation. New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;
- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

This policy 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. It is linked to the following school policies:

- Safeguarding (including radicalisation and extremism)
- Staff Behaviour;
- Health and Safety;
- Anti-Bullying;
- Data Protection;

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Wellesley Prep we understand the responsibility to educate our pupils on e-safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within

the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

SCOPE OF THIS POLICY

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

This policy covers 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.).

ROLES AND RESPONSIBILITIES

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy in conjunction with the child protection policy at least annually. The Governor who is responsible for safeguarding and child protection and e-safety is Alan Winter. This includes the reviewing of our filtering and monitoring infrastructure and processes.
(a.winter@daneshillprepschool.com)

2. Head and the Senior Leadership Team (SLT)

The Head is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Head has delegated day-to-day responsibility to the deputy head, who is the head of pastoral care and DSL.

In particular, the role of the Head and the SLT is to ensure that:

- a. staff, in particular they are adequately trained about e-safety; and
- b. staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

3. E-safety coordinator

The School's head of pastoral care/DSL is responsible to the Headteacher for the day-to-day issues relating to e-safety. He/she has responsibility for ensuring this policy is upheld by all members of the school community, and works with IT staff to achieve this. They will keep up to date on current e-safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP, Childnet International and Hampshire Children's Services. The DDSL/ Head of digital learning plays a key role in ensuring the policy is relevant and accurate.

4. IT staff

The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails, maintain content filters, and will report inappropriate usage to the deputy head, who is also the DSL. (d.bickford@wellesleyprep.co.uk) 07834588639. A filtering and monitoring system recognises any attempts to search for inappropriate material and instant reports are received by the DSL/Head of Digital Strategy. The newly appointed Head of Digital Strategy has a technical overview of the school's hardware and systems, and will liaise with the DSL to ensure the e-safety policy is adequate.

5. Teaching and support staff

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

6. Pupils

Pupils are responsible for using the school IT systems in accordance with the Acceptable Use Policy, and for letting staff know if they see IT systems being misused.

7. Parents and carers

Wellesley Prep School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage.

The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

Parents and carers are responsible for endorsing the school's Acceptable Use Policy.

EDUCATION AND TRAINING

1. Staff: awareness and training

New teaching staff receive information on Wellesley Prep School's e-Safety policy as part of their induction.

All staff and governors are aware of our filtering and monitoring system – what it does and how we deal with any information it provides. This is reviewed annually.

All teaching staff receive regular information and training on e-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 e-safety. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school e-Safety procedures. These behaviours are summarised in the Acceptable Use Policy which must be signed and returned before use of technologies in school. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-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.

A record of concern must be completed by staff as soon as possible if any incident relating to e-safety occurs and be provided directly to the school's head of pastoral care/DSL.

CYBERBULLYING - PREVENTATIVE MEASURES

Mr Bickford (Deputy Headmaster and DSL), Miss Gibson-James (Head of Pre-Prep and DDSL), Mr Jerrold (Head of Digital Strategy and DDSL) and Mr McDonald (Headmaster and DDSL) help to support all staff in ensuring cyberbullying is understood and acted on. The DSL takes responsibility for online safety. The ICT curriculum (as well as PSHE and assembly rota) teaches children to stay safe online.

The children are made aware of the risks posed by adults or young people, who use the internet and social media to bully, groom, abuse or radicalise other people, especially children, young people and vulnerable adults.

Abuse can take place wholly online or technically may be used to facilitate online abuse.

This section is especially relevant when considering the increased online learning from home.

There are four recognised areas of risk online:

- **content:** being exposed to illegal, inappropriate or harmful material;
- **contact:** being subjected to harmful online interaction with other users; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams'
-

On-site, we prevent exposure to these areas of harm with the following measures:

- Every year group is taught about e-safety through the ICT curriculum which covers blocking, removing contacts from 'buddy lists', use of social media and sharing personal data. Rules regarding Responsible Internet Use are clearly displayed.
- An internet filtering and monitoring system (for all pupil log-ins) which blocks all inappropriate content but not to the detriment of effective teaching and learning. All staff understand this, too.
- A total ban on all personal mobile devices (unless children need a mobile for after-school logistics, in which case the phone should be kept in the school office for the day) with the wifi being inaccessible to any user without the appropriate security details.
- All ICT based activities are fully supervised by staff.

- Raising awareness about online safety and cyber-bullying. Pupils are made aware of the fact that the school's responsibility for their welfare does not end at the end of the school day or at the school gates. They know that we expect them to apply the principles of the school's code of conduct to their behaviour online either during their interactions with one another or the wider public. If the school intercepts evidence to the contrary, we will apply our anti-bullying policy and/or rewards and sanctions procedures as if the behaviour took place in person and on-site.

The latest resources regarding online safety promoted by DfE can be found at:

- www.thinkuknow.co.uk
- www.disrespectnobody.co.uk
- www.saferinternet.org.uk
- www.internetmatters.org
- www.childnet.com/cyberbullying-guidance
- www.pshe-association.org.uk
- educateagainsthate.com
- www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Recent tangible examples of the school promoting awareness include: Talks given by DSL/DDSL on "Preparing children for a digital world" twice in 2023. Talks given to pupils in 2021 and 2022 on e-safety from NSPCC (Speak out and Stay Safe) and maintaining a sincere social media profile (for Year 7&8) as they move on. Talks for parents have been given (online) each year from Alan McKenzie and Kidscape. Esafety links and advice sent out at the start of lockdown in March 2020. Intermittent messages are sent to parents surrounding issues we have faced in school, and advice for parents to support children at home. In November 2018 and December 2020 the school completed an online survey, the results of which were discussed and shared with staff, pupils and parents. In March 2016 senior pupils attended a series of conferences including a monologue and workshop on bullying and a presentation on terrorism and extremism. In April 2016 the school formed a partnership with Gooseberry Planet, an online safety app, becoming one of the first prep schools in the country to do so. This coincided with a joint pupil, staff and parent conference about online safety led by Gooseberry planet's CEO. In October 2016, all staff completed Channel Prevent Training online which looks at the danger of online recruitment from extremist organisations. This has been updated each September as part of the whole-staff Safeguarding Awareness Workshops and online training. Each year, safeguarding training for children takes place through the NSPCC. This includes what abuse is, internet safety, raising awareness of our mental health and how to speak out.

SEND Children

It must be recognised that children with SEND are disproportionately more likely to be victims of all types of abuse. This must always be taken into consideration when confronted with information and the DSL should be trained in this.

2. Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-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, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their e-safety responsibilities through the PSHE/ICT curriculum and to look after their own online safety. From year 3 pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL/DDSL/School Independent listener and any member of staff at the school.

Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images (etc.) through PSHE and ICT lessons, in discussion and classroom activities.

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 Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach DSL/DDSL/School Independent listener as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

All school devices leased to children are regularly updated and all controls installed before given to children.

3. Parents

The school seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges discussion evenings for parents when an outside specialist advises about e-safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

POLICY STATEMENTS

1. 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 at Wellesley Prep are permitted to bring in personal devices for their own use. They may use such devices in the staff room but not otherwise around school unless in emergency.

Personal telephone numbers, email addresses, or other contact details may not be shared with pupils or parents / carers and under no circumstances may staff contact a pupil or parent / carer using a personal telephone number, email address, social media, or other messaging system.

Pupils

No personal devices belonging to pupils are to be brought into school or used at school, whether for school work or personal use.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the SENCO to agree how the school can appropriately support such use. The SENCO will then inform the pupil's teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access social networking sites from school devices or whilst in front of pupils. Such access may only be made from staff members' own devices whilst in the staff room.

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.

The school has taken all reasonable steps to ensure that the school network is safe and secure. Staff should be aware that email communications through the school network and staff email addresses are monitored.

Staff must immediately report to the deputy head/DSL 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 deputy head or headmaster.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Wellesley Prep 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.

Under no circumstances should school pupils or parents be added as social network 'friends' or contacted through social media.

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 using any personal email address.

Pupils

Whilst phones are not permitted in school, the school expects pupils to think carefully before they post any information online, or repost or endorse content created by other people. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

Pupils must report any accidental access to materials of a violent or sexual nature directly to the Deputy Head/DSL. Pupils should be aware that all internet usage via the school's systems and its wifi 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 contact the IT Manager for assistance.

3. Data storage and processing

The school takes its compliance with the Data Protection Act 1998 seriously. Please refer to the Data Protection Policy and the Acceptable Use Policy for further details.

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.

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

4. 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.

5. 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 peer-on-peer abuse, cyberbullying, stalking or Child Criminal Exploitation/Child Sexual Exploitation 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 images on the internet (e.g. on social networking sites).

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. However, these images should not be published on blogs or social networking sites (etc.) or even shared with others without permission from parents, nor should parents comment on any activities involving other pupils in the digital / video images.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment: personal equipment should not be used for such purposes.

Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Pupils must not take, use, share, publish or distribute images of others.

Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website.

Photographs published on the school website, or displayed elsewhere, that include pupils, will be selected carefully and will comply with good practice guidance on the use of such images.

Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6. Misuse

Wellesley Prep School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police. If the school discovers that a child or young person is at risk as a

consequence of online activity, it may seek assistance from the Hampshire Children's Services. Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures.

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.

COMPLAINTS

As with all issues of safety at Wellesley Prep School, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Headmaster who will liaise with the governors/SLT and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded by the DSL and raised with the Headmaster. Alan Winter, Governor for Safeguarding and Child Protection Issues will be informed of any such issues too.