SIR WILLIAM PERKINS'S SCHOOL

E-safety

1. Policy Statement

This policy statement applies to all staff, volunteers, children and young people. It is the duty of Sir William Perkins's School (SWPS) to ensure that everyone at the school is safe and in doing so, we will:

- ensure we maintain the safety and wellbeing of children and young people when adults, young people or children are using the internet, social media or mobile devices
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- operate in line with our values and within the law in terms of how we use online devices.

Our students 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

This policy statement should be read alongside our other SWPS policies and procedures, including:

- Safeguarding and Child Protection
- Anti-Bullying
- GDPR and Privacy notices
- Good Behaviour Policy
- Discipline and Exclusions Policy
- Digital Media Policy
- Health and Safety Policy

- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti bullying policy
- IT Acceptable Use Policy
- Use of Images Policy

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 Sir William Perkins's School, we understand the responsibility to educate our students 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 students in discussions about e-safety and listening to their fears and anxieties as well as their thoughts and ideas.

SWPS is fully committed to ensuring that the application of this policy is non-discriminatory, in line with UK Equality Act (2010). Further details are available int eh school's Equal Opportunities policy.

2. Scope of this Policy

This policy applies to all members of the school community, including staff, students, 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 students, carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the Acceptable Use Policy for all staff, visitors and students 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 students, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, smart watches etc.).

3. Roles and responsibilities

3.1 The Governing Body

The governing body of SWPS is responsible for the approval of this policy and for reviewing its effectiveness. It is the role of the safeguarding governor to ensure that the e safety policy is in place in conjunction with the Deputy Head Pastoral, the Deputy Head Staff, Co-curricular and Compliance, and the member of staff with responsibility for e-safety.
Governor training for online safety is through National on-line Safety (school membership).

3.2 Headteacher and the Senior Leadership Team

The Headteacher is responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Headteacher has

delegated day-to-day responsibility to the e-safety coordinator and designated safeguarding leads.

In particular, the role of the Headteacher and the Senior Leadership Team is to ensure that:

- staff, in particular the e-safety coordinator are adequately trained and up to date on e-safety
- 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.

3.3 E-safety coordinator

The school's e-safety coordinator is responsible to the Deputy Head Pastoral for the day-to-day issues relating to e-safety. The e-safety coordinator 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 (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

3.4 Prime Networks

The school's IT support staff (Prime Networks) have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast of 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 Designated Safeguarding Lead or Headteacher.

3.5 Teaching and support staff

All staff are required to sign 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 e-safety issues which may arise in classrooms on a daily basis.

3.6 Students

Students are responsible for using the school IT systems in accordance with the IT Acceptable Use Policy and for letting staff know if they see IT systems being misused. All students must also have read and agreed to the Mobile Device Policy.

3.7 Parents and carers

Sir William Perkins's School believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We 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 student 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 IT Acceptable Use Policy and Mobile Device Policy.

3. Education and training

3.1 Staff: awareness and training

New teaching staff receive information on Sir William Perkins's School's e-safety and IT Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training or an Educare online course and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety. All supply staff and contractors are expected to complete a safeguarding course that includes e-safety.

All staff are responsible for demonstrating, promoting and supporting safe on-line behaviours and following school e-safety procedures.

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.

All staff 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 on CPOMS (Child Protection Online Management System) as soon as possible if any incident relating to e-safety occurs and be provided directly to the appropriate members of the Pastoral Team and Designated Safeguarding Lead.

3.2 Students: e-safety in the curriculum

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

The school provides opportunities to teach about e-safety within some curriculum areas including PSHCE and Computer Science. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via PSHCE, by presentations in assemblies, during E Safety Week as well as informally when opportunities arise.

At age-appropriate levels, and usually via PSHCE, students are taught about their e-safety responsibilities and to look after their own online safety. From Year 8, students are formally 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. Students can report concerns to the pastoral team, the e-safety Coordinator and any member of staff at the school.

Students are also taught about relevant laws applicable to using the internet such as data protection and intellectual property. Students are taught about respecting other people's information and images, through discussion and classroom activities.

Students are made aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues. Students should approach the pastoral team as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

3.3 Parents/carers

The school seeks to work closely with parents/carers in promoting a culture of e-safety. The school will always contact parents/carers if it has any concerns about students' 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/carers may feel equipped to protect their child when they use electronic equipment at home. All parents are given the National Online Safety membership through the school which includes plenty of information on e-safety.

4. Use of school and personal devices

4.1 Students

If students in the lower years bring in personal mobile devices they will be collected in at morning registration and handed back at afternoon registration.

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

5. Use of internet and email

5.1 Staff

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.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Sir William Perkins's 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 students or parents be added as social network 'friends' or contacted through social media by staff.

Any digital communication between staff and students or parents / carers must be professional in tone and content. Under no circumstances may staff contact a student or parent / carer using any personal email address.

5.2 Students

Students 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 the pastoral team or another member of staff.

The school expects students 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.

Students must report any accidental access to materials of a violent or sexual nature directly to their Head of Year or another member of staff. Deliberate access to any inappropriate materials by a student will be dealt with under the school's Good Behaviour Policy.

The school instructs students to exclusively use the school's network to access the internet in order for the robust filtering and monitoring system to protect them from harmful content.

6. Safe use of digital and video images

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, parents / carers and students 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 students about the risks associated with the taking, use of, sharing of, publication of and distribution of images.

In particular they should recognise the risks attached to publishing their own images on the internet.

Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow this policy, the Digital Media policy and the Use of Images 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 students are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

Consent from parents or carers will be obtained as outlined in the Use of Images policy.

Photographs published on the school website, or displayed elsewhere, that include students, will be selected carefully and will comply with good practice guidance on the use of such images. Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

7. Misuse

Sir William Perkins's School will not tolerate illegal activities or activities that are inappropriate in a school context, and will report illegal activity to the police and/or the LSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP and make a referral to Children's Services, in line with the Safeguarding and Child Protection policy.

The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Anti-Bullying Policy and Discipline and Exclusions Policy.

8. Complaints

As with all issues of safety at Sir William Perkins's School, if a member of staff, a student or a parent / carer has concerns relating to e-safety prompt action will be taken to deal with it. Concerns should be addressed to the e-safety coordinator in the first instance, and will be dealt with in accordance to the school's Complaints Policy as appropriate.

Incidents of, or concerns around e-safety will be recorded using CPOMS and reported to the school's e-safety Co-ordinator and the Designated Safeguarding Lead, in accordance with the school's Child Protection Policy.

9. Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children in England. On this basis:

We believe that:

- children and young people should never experience abuse of any kind

- children should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

We recognise that:

- the online world provides everyone with many opportunities; however, it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using the network or devices at Sir William Perkins's School.
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety
- all children, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse.

We will seek to keep children and young people safe by:

- appointing an e-safety coordinator
- providing clear and specific directions to staff and volunteers on how to behave online
- supporting and encouraging all young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents or carers
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour.
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.

If online abuse occurs, we will:

- Following clear and robust safeguarding procedures
- Provide additional support and training for all staff and volunteers in e-safety

- Ensure our responses take into account the needs of the person experiencing abuse
- Review the e-safety policy regularly to ensure we are up to date

10. Monitoring and Review

The Governing Body is ultimately responsible for the effective oversight, review and amendment of the is policy and understand its legal obligation to do so.

This document will be reviewed and updated annually by the E-safety co-ordinator or as events or legislation requires.

Next scheduled review date: March 2025 Last reviewed: March 2024	
Key updates in this version:	• Minor updates to content and layout to aid clarity.