SOLIHULL

Online Safety Policy and Curriculum Document

Owner: DSL Pastoral Support Manager
Reviewer: Assistant Head (Digital Learning and ICT Strategy)
Last Reviewed: September 2023

Version 4

Policy Statement

We need to protect our pupils when they are in our care and educate them for when they are not.

The Internet and technology in general are essential tools in the education of our pupils to play a role in a modern, technologically diverse society. It should be used to raise educational standards, encourage independent research, promote collaboration and enable remote learning where appropriate. Pupils use the Internet widely outside of schools, and the advent of online platforms such as Microsoft Teams and the Media Server extend the learning environment beyond the classroom.

There has been an increasing focus on Online and E-Safety in recent years and attention has been drawn to the need for all children and young people to be given the skills and knowledge they need to keep themselves safe when using new technology. Many parents and carers currently feel unable to do this adequately, often because they feel they lack the necessary information. Online Safety also forms part of the safeguarding arrangements that schools should have in place to protect the children and young people in their care. At Solihull School, we have a duty to teach Online Safety to all pupils, and to invite parents to information evenings to discuss the use of technology and how they can assist in keeping their children safe.

The themes to address can be categorised into one of four areas of risk as identified in Keeping Children Safe in Education (2022):

- Content - being exposed to illegal, inappropriate or harmful material (1)
- Contact - being subjected to harmful online interactions (2)
- Conduct - personal online behaviour that increases the likelihood of, or causes, harm
- Commerce – risks such as online gambling, inappropriate advertising, phishing and financial scams. Pupils, students or staff are at risk, can be reported to the Anti-Phishing Working Group (**https://apwg.org/**).

Policy Aim

The Online safety policy sets out how the school prepares pupils to use technology responsibly and safely.

Management of Online Safety

The following members of staff have a responsibility in the management and implementation of Online Safety.

Mrs Sarah Hardy (DSL / Pastoral Support Manager)
Mr Matthew van Alderwegen (Assistant Head: Digital Learning and ICT Strategy)
Mrs Louise Rooney (Head of Wellbeing and Personal Development/Anti-Discrimination Lead) *
Mrs Vanessa Patel (Head of Computer Science)
Mr Michael Jones (Senior Deputy Head of Prep School: Pastoral & Staff Welfare)
Mrs Alex Longden (ICT Subject Leader for Prep School)
Mr Martin Moseley (Head of Technical Support)
Deputy Designated Safeguarding Leads – See Safeguarding & Child Protection Policy

**CEOP Ambassador*

Associated Policies

A range of policies are associated with Online Safety. Please refer to the Policies Folder in 'Staff Only' where the following policies are stored.

ICT Acceptable Use Policy
Staff Mobile Telephone and Photography Protocols
Safeguarding and Child Protection Policy
Social Networking Policy
Wellbeing and Personal Development Policy

Protective Measures

Prevention: In accordance with *'Prevent'* guidance, pupils have filtered online access via our network, whether they do so from a school owned computer or by one of their own devices connected to our network via the Wi-Fi. All connections to the Internet from our network go through a web filter, which restricts access to websites and content deemed unsuitable for young people, including extremist websites, social media, pornography, racism and bullying. This includes access to messenger facilities of these sites [(2)]. The filter is updated several times every day (e.g. Incel terminology), and websites can be added to a white list or black list in addition to this. By request from a member of staff, a website can be added to our white list and thus making it accessible, but only after reasonable checks about the suitability of the content. YouTube is blocked, apart from content categorised as 'educational' by YouTube. The School's media server acts as a walled garden for content deemed suitable for use in the education of our young people. It is made explicit to pupils in the Acceptable Use Policy that pupils should never tether their laptops to mobile devices as a means of bypassing these safeguards.

Monitoring: A report can be generated on any user's online activity, including date and time of visit to specific sites. As part of the induction of new pupils and staff, the Acceptable Use Policy is addressed and discussed in order that pupils are aware of the dangers of the technology, our expectations of pupils and staff as a user, and the consequences of breaching the AUP. Users are aware that their use of the Internet is monitored, and that discretion and appropriate conduct is essential. This is reinforced throughout the curriculum. Through their use of technology within ICT lessons and elsewhere in the curriculum, pupils will learn to remain within the parameters allowed by our policy, and to report any abuse or unsuitable content that they encounter. They will learn to be productive online and how to distinguish between search results that are likely to be useful vs those which may be less accurate or reliable.

An IT filtering system (SMOOTHWALL) is in place to keep children safe when accessing the internet at school. The system also filters on search terms and also allows for terms to be added for filtration purposes, e.g., the words/terms used in extremism propaganda (which have been added) in line with the Prevent Duty requirements. Smoothwall is updated daily and the school refer alerts to The Designated Safeguarding Lead or Deputy Designated Safeguarding Lead, log incidents/concerns on CPOMS and hold summative data for review.

Safeguarding and Education: Each user has an email address within the domain of solsch.org.uk and only this email address plus 'posts' and direct 'chat' communications within Teams must be used by staff in communicating with pupils. Chat discussions within Teams are fully searchable. Pupils are taught about 'netiquette' and how to use email and chat functions responsibly as part of their ICT curriculum, alongside what is responsible and irresponsible email communication, relating to safeguarding and Online Safety. Pupils are told that staff have access to their email mailboxes as part of the Acceptable Use Policy. Pupils are taught in WPD and Computing lessons on how to protect themselves and others online. This is revisited and reinforced each year with Safer Internet Day involving whole school assemblies, pupil surveys and sharing feedback on key and contemporary issues relating to online safety.

Protection: All school owned devices including servers are fitted with up-to-date anti-virus software (currently Sophos), and any incoming content passes through a firewall and filter. Pupils in the Middle School and Sixth Form who bring their own devices (BYOD) to school are instructed to access school WiFi which also passes through this filter and are instructed that they are not to tether their laptops to their mobile phones.

Video conferencing with eternal organisations only take place during planned sessions as dictated by the organising member of staff, and pupils are supervised at all times. The IP address of the video conferencing camera is not published, and only the planned partner is given the details. Such sessions are with respected professional organisations including museums, and use the School's leased-line connection. In the unusual event of recordings being made, these are authorised by both parties beforehand. When not in use, the camera is unplugged from mains and network.

The use of mobile phones in lesson time is not allowed except with the express permission of the member of staff. This is referenced under the AUP (Acceptable Use Policy) and was reviewed in the light of our Bring Your Own Device (BYOD) policy.

The AUP is posted on our website and Parent Portal, parents receive a copy when their children first start and pupils are reminded that they must agree to be bound by the terms and conditions. The AUP is also on display in the ICT Classrooms.

Protection of Personal Data and Sensitive Content Online.

Each year, the Assistant Head: Digital Learning and ICT Strategy delivers a talk to the whole staff on data security covering elements such as compliance with the Data Protection Act 1998 and GDPR 2018, keeping pupil data secure, and best practice, as well as informing of our measures in place to ensure data is kept secure. These include password enforcement policy, currently a minimum of 8 characters, with the last 5 passwords cannot be re-used, and a lock out period of 3 days if a user enters the password incorrectly 10 times. In the past 12 months 2 Factor Authentication has also been introduced to provide an extra layer of protection to data.

Personal data on pupils is housed on our MIS, iSAMS, which requires a secure login. Not all staff have access to all data, and items of a particularly sensitive nature relating to safeguarding are kept on a database that is not available online. The more recent use of the iSAMS App by staff also means personal data is available to staff on mobile devices. Mobile phones require a key code, touch or face ID to access to unlock the

phone and access the application. All personal data is backed up on iSAMS every day and archived every half term to hard drive, which is kept for 7 years.

Content on school platforms (e.g. Microsoft Office 365) is only accessible to authenticated users. Parents cannot see lesson material directed to pupils, and pupils cannot see the Parents section, devoted to matters such as consent for trips and visits. General policies such as the school's Anti Bullying Policy, Behaviour and Discipline Policy, Data Protection Policy and the Safeguarding and Child Protection Policy can be found on the portal and website for Parents and on the school's website **http://www.solsch.org.uk** .

Our website and social media sites do include photographs of current pupils. The permission of parents is sought before any photographs are used. Pupils are not normally identified by their full names. Such photos are always considered with care, and only appropriate ones are posted. Any posts made by members of staff on our website or social media sites are done by and on behalf of the school, and as such, personal opinions and comments are not posted. They are usually directed through the Marketing Manager. No personal details are posted, apart from contact email addresses for admin purposes. Teachers may run blogs within our school platforms, but these are for educational and school purposes. No personal social media content is permitted.

Online Safety Curriculum

1. Aims

- To keep children and young people safe from predatory adults.
- To help children and young people avoid physical danger.
- To help children safe from sexual violence and harassment online.
- To help children and young people avoid becoming victims of crimes such as identity theft and fraud
- To help children and young people avoid embarrassment or humiliation.
- To develop responsibility in their use of the Internet.
- To help children and young people develop the skills to use information wisely and well.
- To help them avoid harmful behaviours such as obsessive use of the Internet or digital games

Children and young people are often capable of using safe strategies, but we need to be sure that they know what to do to stay safe online. Many young people have the technical skills to deal with Online Safety, but they sometimes lack the wisdom to know when there is danger or how to deal with difficult situations. Adults (teachers and parents and carers) are sometimes over-cautious or over-protective in their responses to these dangers. The Byron reviews highlight the need to help children and young people tackle these issues rather than keep them protected from them and therefore prevent them learning how to deal with issues that arise. Our policy is one of educating and monitoring, whilst blocking the most harmful, offensive or illegal activities.

2. Curriculum

Online Safety is a broad description covering a range of aspects including, but not limited to the 4 C's set out in Keeping Children Safe in Education (2022).

- Content - being exposed to illegal, inappropriate or harmful material, as well as, bias and unreliable information.
- Contact - being subjected to harmful online interactions that come about because of communication possibilities that the internet provides.
- Conduct - personal online behaviour that increases the likelihood of, or causes, harm and illegal behaviour related to copyright and technical issues such as filtering.
- Commerce – risks such as online gambling, inappropriate advertising, phishing and financial scams. Pupils, students or staff are at risk, can be reported to the Anti-Phishing Working Group (**https://apwg.org/**).

The term Online Safety therefore covers a broad range of aspects including physical safety, legal aspects such as copyright and technical issues such as filtering, as well as becoming a responsible digital citizen, informed of risks and dangers of their online activities.

We use some of the resources available as staff trained by CEOP which are kept behind a secure login. These cover topics such as sharing nudes and semi nudes online (sexting), grooming and social media posts. Whilst pupils do not have access to social media sites from within school as part of the AUP, and enforced by our web filtering, it is recognised that they may well access these outside of school, so we believe that education of their responsible use is a cornerstone to their safety and wellbeing. The content covers responsible use of social media and privacy settings, as well as reporting offensive online behaviour by others.

When and how online safety is taught at Solihull School.

Most teaching of Online Safety in the School will be taught through ICT, Wellbeing and Personal Development lessons and year-group specific assemblies. Online Safety aspects are built into the schemes of work which are for discreet ICT lessons in the Prep School, and from Thirds to Fourths. These activities, alongside activities in the Wellbeing and Personal Development curriculum and in other subjects, which involve use of internet-based content, provide the means of delivering the Online Safety curriculum. Teachers also use opportunities throughout the curriculum to reinforce safe Internet use and to deal with issues such as evaluating information.

Teaching online safety is progressive and topics are dealt with at times relevant to the age of the pupils. The Senior School programme builds upon that delivered in the Preparatory School. Responsibility - and with it the freedom to explore - should increase with improving knowledge and skills and support the Spiritual, Moral, Social and Cultural (SMSC) development of all of our pupils. The curriculum can be adapted to addressing emerging internal and external concerns.

At Solihull School the teaching of online safety has at its heart the Acceptable Use Policy, which all pupils (and their parents) are required to agree to before they use the school's ICT facilities. The Wellbeing and Personal Development curriculum includes aspects relating to online/cyber- bullying using technologies such as emailing, mobile phones, social networking sites etc. The School participates in Safer Internet Day annually. Assemblies and activities linked to this and Anti-Bullying Week are key aspects of our Co-Curricular and Pastoral provisions.

Many safety issues we address in school rely on a partnership with our parents and carers whom we encourage to be actively involved in helping their children to stay safe at home as well as at school. Schools have responsibility for working with parents and carers to deal with incidents of bullying (inc. cyber/online bullying) using new technologies that happen outside school, where those incidents involve two or more pupils from the same school. The introduction of an Online Safety curriculum provides an opportunity to talk to parents and carers and to develop a working partnership with them in Online Safety matters. Solihull School parents and carers have in the past been pointed in the direction of Online Safety information on the Internet and/or invited to Online Safety events at school, and will continue to have this supported provided. Key staff have been CEOP trained and are qualified to deliver the training materials. At the Preparatory school Mrs A Longden has been CEOP trained and qualified. Mr. M van Alderwegen has also covered the CEOP training.

The development of Microsoft Teams provides opportunities to teach Online Safety by including safe instant communication areas (e.g Teams Chat) for pupils but which will not be accessible to the public. These technologies allow us to enhance the teaching of safe behaviours when using chat, blogs and discussion forum.

There is a balance to be struck, particularly with young children, between encouraging the safe use of ICT and making children fearful. The aim is not to discourage use of ICT but to give children the experience, skills and knowledge to use it sensibly and safely. The Internet is a powerful and exciting tool and, used with safety guidelines in place, provides many very positive academic and pastoral benefits to our pupils.

Other matters are covered by the AUP which are not a direct part of Online Safety such as copyright legislation, plagiarism and using the facilities responsibly.

Online Safety Curriculum

Preparatory School:

Pupils are taught a discreet online safety curriculum, which complements the Acceptable Use Policy for Solihull Preparatory School. Most teaching of online safety in the Preparatory School will be taught through PSHEE, Computing, and year-group specific assemblies.

Teachers will also use opportunities throughout the curriculum to reinforce safe Internet use and to deal with issues such as evaluating the reliability of information and other digital literacy skills.

Pupils and their parents sign up to the Preparatory School's Rules for Responsible Internet Use before they can use the school's ICT facilities, copies of which are displayed in the Prep school's ICT Suites. These rules are reinforced by all Preparatory School staff who use ICT in their lessons.

Senior School

Online, E-Safety and over-arching Digital Citizenship is embedded into the Wellbeing and Personal Development Curriculum, Computer Science Lessons, Whole School and Sectional Assemblies and academic lessons.

Thirds Computer Science Lessons:

Staying safe online – issues such as keeping personal information private, not unwittingly revealing this to a Third Party and awareness that people online may be dishonest about what they are / their intentions. Use of Social Media and Chat rooms / IM

Shells Computer Science Lessons:

Social networking, online/cyber bullying, cyber blackmailing, sharing nudes and semi-nudes online (sexting), reporting abuse and staying safe. The digital footprint that is left. Many resources provided by CEOP are embedded in our curriculum. Social media is specifically covered here, as children need to be 13 to have an account (although many children the world over lie about their ages) including privacy settings and reporting abuse. References to Childline, CEOP and ThinkUKnow sites. Dangers of excessive use of technology include internet gaming and associated health risks RSI, headaches, DVT etc

Fourths Computer Science Lessons:

Chat room and IM Chat safety, sharing nudes and semi nudes online (sexting), cyber/online bullying and reporting abuse [2,3]. Password security, hacking and phishing. Again, sharing personal information is covered, and the likelihood of someone being dishonest in order to gain what they want from a young person. Saving evidence and reporting are particularly emphasised at this stage, along with the dangers of meeting up in real life with someone they have met online. Cyber blackmailing is also covered, and safe use of mobile phone (avoiding mugging etc).

N.B. Computer Science is an optional subject in the Lower Fifth and Upper Fifth. The teaching of online safety is imbedded in the Wellbeing and Personal Development beyond this point.

Parents:

Information about Online Safety is offered regularly for parents in the Preparatory and Senior School at key points in the year (e.g. the end of the Summer Term). Themes broadly follow the annual themes set out for Safer Internet Day by UK Safer Internet Centre, as well as reviewing the four areas of risk on the internet,

safeguarding, new technology, new software and giving parents the opportunity to ask questions and have an open dialogue with the school.

Schools will communicate annually with parents about:

• what systems the school have in place to filter and monitor online use

• what the school are asking children to do online, including the sites they will asked to access

• who from the school their child is going to be interacting with online

Information and Support

Refer to KCSIE Online Information for more information to support schools to keep children safe online.

Acknowledgements:

The development of this document has involved looking at the work of a number of agencies and local authorities including the following:

West Midlands Regional Broadband Network (WMNet)
http://www.wmnet.org.uk

The London Grid for Learning (LGfL)
http://www.lgfl.net/esafety/Pages/policies-acceptable-use.aspx

Think U Know
https://www.thinkuknow.co.uk/

Child Exploitation and Online Protection
https://www.ceop.police.uk/safety-centre/

Department for Education
Teaching Online Safety in Schools - June 2019 – Last updated Jan 2023

Department for Education
'Keeping Children Safe in Education' 2023 – September 2023

The Safer Internet Centre
https://www.saferinternet.org.uk/