E-Safety (Senior School) Policy

Ref: ***LP-PS-013***	Version: ***5.10***	Date: ***10th August 2023***
Document Owner: ***Emma Parsons (Deputy Head - Pastoral)***		
Description: This policy outlines the Senior School's approach to e-safety.		

OUR SCHOOL AIMS

- *To be a safe and trusted foundation for our pupils to achieve their individual academic, social and creative potential.*
- *To cultivate the skills, knowledge, self-awareness and academic credentials our pupils will need to confidently meet the challenges of our rapidly changing world.*
- *To instil and nurture a strong sense of social responsibility, integrity and environmental awareness so our pupils positively contribute to a sustainable and just society.*
- *To guide each pupil in the discovery, delight and development of their individual gifts, talents and character.*
- *To create and sustain an inclusive and contemporary school culture, where diversity, difference and individuality are recognised and celebrated.*
- *To prioritise physical and emotional wellbeing across every facet of our school community.*

1.0 INTRODUCTION

1.1 We believe this policy should be a working document that is fit for purpose, represents the school ethos, enables consistency and quality across the school and is related to the following legislation:

- Obscene Publications Act 1959
- Children Act 1989
- Computer Misuse Act 1990
- Education Act 1996
- Education Act 1997
- Police Act 1997
- Data Protection Act 2018
- Human Rights Act 1998
- Standards and Framework Act 1998
- Freedom of Information Act 2000
- Education Act 2003
- Children Act 2004
- Safeguarding Vulnerable Groups Act 2006
- Education and Inspections Act 2006
- Children and Young Persons Act 2008
- School Staffing (England) Regulations 2009
- Equality Act 2010
- Education Act 2011
- Protection of Freedoms Act 2012
- Counter Terrorism and Security Act 2015

1.2 The following documentation is also related to this policy:

- Dealing with Allegations of Abuse against Teachers and other Staff: Guidance for Local Authorities, Headteachers, School Staff, Governing Bodies and Proprietors of Independent Schools (DfE)
- Equality Act 2010: Advice for Schools (DfE)
- Keeping Children Safe in Education: Statutory Guidance for Schools and Colleges (DfE)
- Prevent Strategy (HM Gov)
- Teaching approaches that help build resilience to extremism among people (DfE)
- Working Together to Safeguard Children: A Guide to Inter-agency Working to Safeguard and Promote the Welfare of Children
- Race Disparity Audit - Summary Findings from the Ethnicity Facts and Figures Website (Cabinet Office)

1.3 The School (Lingfield College, Lingfield College Prep, Lingfield Nursery, Lingfield Sixth Form) recognises that technology plays an important and positive role in children's lives, both educationally and socially. It is committed to helping all members of the school community to understand both the benefits and the risks, and to equip children with the knowledge and skills to be able to use technology safely and responsibly.

1.4 The e-Safety Policy relates to other policies including those focused on cyberbullying, anti-bullying, behaviour management and for child protection. Please see other policies connected with e-Safety listed at the end of this document.

1.5 The Senior School's e-Safety Co-ordinator is the Deputy Head (Pastoral), who is also the Designated Safeguarding Lead.

1.6 This e-Safety Policy has been written by the Senior School, building on best practice and government guidance. It has been agreed by Senior Management and approved by Governors. The Policy and its implementation are reviewed annually.

1.7 It is essential that children are safeguarded from potentially harmful and inappropriate online material. Keeping Children Safe in Education 2023 gives guidance on the subject of online safety in schools:

'It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.'

1.8 The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your students, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/). (KCSiE 2023)

2.0 TEACHING AND LEARNING

2.1 The internet is an essential element in 21st century life for education, business, and social interaction. The School has a duty to provide students with quality internet access as part of their learning experience. However, the benefits of internet access are tempered by its inherent risks, and the School is of course aware that all of its members, whether staff, parents or students, rely increasingly heavily on the digital world. It is a valuable tool for teaching and research, but the rules to infringe abuse need to be stringent and frequently reviewed.

2.2 We believe all pupils and other members of the school community have an entitlement to safe internet access at all times.

Key e-safety messages:

Children need to be guided on:

- the benefits and risks of using the internet
- how their behaviour can put themselves and others at risk
- what strategies they can use to keep themselves safe
- what to do if they are concerned about something they have seen or received via the internet
- who to contact to report concerns
- that they won't be blamed if they report any e-Safety incidents
- that cyberbullying cannot be tolerated
- the basic principles of how to behave on the internet.

2.3 Staff are aware that some children may be more vulnerable to risk from internet use, generally those children with a high level of computer skills but coupled with poor social skills.

- The internet use is a part of the statutory curriculum and a necessary tool for staff and students. The VLE Firefly (plus the Firefly app for smartphones or tablets) is used extensively throughout the School curriculum, providing a central base for assessment / revision guidance, class notes & PowerPoints, examination specifications and other resources for remote learning.
- Students will be taught what internet use is acceptable and what is not and given clear objectives for internet use. E-safety is taught as part of the PSHE programme in an age-appropriate way. This is addressed each year as students become more mature, and the nature of newer risks is identified.

- Students are educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval, and evaluation. Students are also shown how to publish and present information appropriately to a wider audience, and to be critically aware of the materials they read before accepting its accuracy.
- Students are taught how to report unpleasant internet content e.g. using the CEOP Report Abuse icon, which can be found on the homepage of the School website.
- The School's Computer Usage Policy is given in full at the point of log-on for every student and member of staff (please see the School's *Computer Usage Policy*)
- The students will have to read through the Use of ICT and Mobile Phone Policy which is in the Student Code of Conduct with their form tutor. This will be set on Firefly as a task, and they will have to click to complete the task and agree to abide by the rules. Within this there is advice about staying safe online.
- The School's internet access is provided by Zen Internet, which is then filtered by the schools firewall SENSO to filter network traffic appropriate to the age of students.
- The School seeks to ensure that the use of internet-derived materials by staff and by students complies with copyright law.
- The PSHE Co-ordinator is a trained CEOP Ambassador, and they provide staff with INSET training on E-Safety. Outside speakers such as Childnet also provide staff INSET sessions to cover different aspect of E-Safety.

MANAGING INTERNET ACCESS

3.0 INFORMATION SYSTEM SECURITY

3.1 All members of staff have their own personal username and password which should be kept private. When a member of staff leaves the School their account is disabled. Computers in school lock after a short period of inactivity to prevent access from unwanted people.

3.2 Staff accessing school systems at home take responsibility for ensuring they are using a secure computer. The Authenticator App is used for offsite access as an additional layer of security. Computers logged into school systems should not be left unattended and when staff have finished working, they must log out of all school systems to prevent unwanted access. Staff are encouraged to use One Drive and Sharepoint on the school system to access files at home rather than carry data on memory sticks which can become lost.

- Staff and students are expected to change their passwords on a 3 monthly basis.
- School ICT systems security is reviewed regularly.
- Virus protection is updated regularly.
- Security strategies are discussed with the internet provider
- iSAMS, the school's information system, is cloud based and backed up externally by iSAMS.

4.0 SCHOOL SYSTEMS

4.1 The Governors recognise that they are expected to do all they reasonably can to limit children's exposure to the risks posed by the internet and ensure that the school maintains appropriate filters and monitoring systems to prevent children from accessing harmful or inappropriate material from the school's IT system.

- The Senso alerting filter is in place to identify those students who may be trying to access harmful and inappropriate material online – a log of blocked searches made on the school system is checked by the Senior and Prep School DSLs on a daily basis.
- The IT technicians will inform the DSL of any harmful and/or inappropriate searches as quickly as possible (within a couple of hours).
- The filtering is based on a category system, and there are blocks on the categories that are deemed inappropriate for school use. In line with government advice and the Prevent Strategy, these blocks include categories regarding terrorist and extremist material.

  Senso is a cloud-based application that monitors classroom computers and students' teams chats. It logs activity such as keywords, visual threats, and phrases. The software is also in line with Ofsted guidance and takes keyword libraries from leading charities such as the Internet Watch Foundation and the Counter-Terrorism Internet Referral Unit. The lists are updated twice a month. Iboss is our web filter, this auto categorises websites and blocks pages depending on the categorisation. Similar to Senso, it also reports certain keywords. This is tested quarterly using: http://testfiltering.com/test/ to ensure it blocks Adult Content, Child Sex Abuse and Terrorism Content efficiently.
- Libra ESVA is our email filter; it uses a combination of AI and keyword lists to ensure the Staff and students don't receive any illicit or dangerous emails.

4.2 All web traffic is logged and monitored. If the content is on the blocked list, an 'access denied' page is displayed. If something inappropriate is accessed on the school computers, it must be reported immediately by a member of staff to the ICT Engineers who will then review the usage log and block the inappropriate conduct. Every day, the Deputy Head (Pastoral) is sent a log of any searches made by staff or students that has been blocked, and where relevant students and parents have been contacted to discuss the nature of such searches.

4.3 The school system is protected by an anti-virus system which scans all files on access, both which are stored on our system and also those on USB pens. Emails are scanned when they are received for inappropriate language, spam, and dangerous attachments. Spam and emails with inappropriate language are blocked and dangerous attachments are stripped from emails. The ICT Engineers regularly monitor the quarantined mailbox, and anything that has gone in here unnecessarily can be released.

4.4 Email

When using email, students are taught:

- not to disclose personal contact details for themselves or others
- to tell their parent or carer immediately if they receive an offensive or distressing email
- not to use email to bully or harass others
- be wary of opening attachments where they are unsure of the content

- E-safety posters are displayed in the IT rooms, Sixth Form computer areas and all form rooms.
- Students and staff may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive an offensive e-mail.
- Students are advised not to reveal personal details about themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- Staff to student communication can take place via email or Teams. Emails must take place via a school email address or from within Firefly and will be monitored. Teams can be used for communication but must only be used during school hours (8am- 5pm), this is monitored.
- External incoming e-mails should be treated as suspicious, and attachments not opened unless the author is known.

5.0 PUBLISHED CONTENT AND THE SCHOOL WEBSITE

5.1 The contact details on the website are the school address, email, and telephone number. Staff or students' personal contact information is not published.

5.2 The Headmaster or nominees take overall editorial responsibility and ensures that content is accurate and appropriate.

6.0 SOCIAL NETWORKING

When using social networking sites, students are taught:

- not to give out personal details to anyone online that may help to identify or locate them or anyone else
- not to upload personal photos of themselves or others onto sites and to take care regarding what information is posted
- how to set up security and privacy settings on sites to block unwanted communications or deny access to those unknown to them
- to behave responsibly whilst online and keep communications polite
- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken`

When using chat rooms, students are taught:

- not to give out personal details to anyone online that may help to identify or locate them or anyone else
- to only use moderated chat rooms that require registration and are specifically for their age group
- not to arrange to meet anyone whom they have only met online
- to behave responsibly whilst online and keep communications polite
- not to respond to any hurtful or distressing messages but to let their parents or carers know so that appropriate action can be taken that any bullying or harassment via chat rooms or instant messaging may have serious consequences

6.1 The School will control access to social networking sites and consider how to educate students in their safe use e.g. use of passwords. This control may not mean blocking every site; it may mean monitoring and educating students in their use.

6.2 Students are advised never to give out personal details of any kind which may identify them or their location.

- Students must not place personal photos on any social network space provided in Firefly.
- Students and parents are advised that the use of social network spaces outside school brings a range of opportunities; however, it does present dangers for users.
- Students are advised to use nicknames and avatars when using social networking sites

7.0 MANAGING FILTERING

7.1 If staff or students come across unsuitable online materials, the site must be reported to the E-safety Coordinator (Deputy Head - Pastoral).

7.2 Senior School staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective, and reasonable.

7.3 A log of any incidents is maintained to identify patterns and student behaviour.

8.0 MANAGING EMERGING TECHNOLOGIES

When using web cameras, students are taught:

- to use them only with people who are well known to them
- not to do anything that makes them feel uncomfortable or embarrassed
- to tell their parents or carers if anyone is trying to force them to do something they don't want to do.

- Emerging technologies will be examined for educational benefit and potential risks assessed.
- Mobile phones and associated cameras are not be used during the school day (8.30-3.50), and students are expected to switch off their phones during these hours and keep them secure (See Mobile Phone policy).
- The use of smartphone cameras is carefully monitored when they are used by students in Photography Club and Media Studies, and they are given guidance on appropriate behaviour.
- It is recognised that such hand-held devices may well not have any form of internet filtering.
- The sending of abusive or inappropriate text messages is forbidden.
- Wherever possible, staff will use a school phone where contact with students is required.
- The appropriate use of Firefly, laptops and alternative learning platforms is discussed as the technology and resources become available within the school.
- Staff use of mobile devices is restricted during the school day when they are around students, and reference is made to this in the Staff Code of Conduct, the Staff Safe Working Practices Agreement and Mobile Phone policy.

9.0 PROTECTING PERSONAL DATA

Personal data is recorded, processed, transferred, and made available according to the Data Protection Act 1998.

10.0 AUTHORISING INTERNET ACCESS

10.1 All staff must read and sign the technology sections of the Staff Code of Conduct before using any school ICT resources.

10.2 The School maintains a current record of all staff and students who are granted access to school ICT systems.

10.3 Students and staff apply for internet access individually by agreeing to comply with the Acceptable Internet Use statement when they log on to any school computer or device.

11.0 ASSESSING RISKS

11.1 The School will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The School cannot accept liability for the material accessed, or any consequences of internet access.

11.2 The School monitors ICT use to establish if the e-safety policy is adequate and that the implementation of the e-Safety policy is appropriate and effective.

11.3 Students who are permitted to use laptops in both internal and external examinations because of SEND needs are expected to complete a formal agreement that addresses issues surrounding illicit access to the internet during examinations. Failure to comply with the School rules can result in students losing their right to use a laptop or access the internet in school.

11.4 Software is installed on the school network which enables staff to monitor the computers being used in a classroom. Staff can view what each student is doing with the exception of passwords.

12.0 CYBERBULLYING

12.1 Cyberbullying is defined as the use of IT to deliberately hurt or upset someone. Unlike traditional physical forms of bullying, the internet allows bullying to continue past school hours and invades the victim's home life and personal space. It also allows distribution of hurtful comments and material to a wide audience.

12.2 Cyberbullying is extremely prevalent as children who would not consider bullying in the physical sense may find it easier to bully through the internet, especially if it is thought the bullying may remain anonymous. In extreme cases, cyberbullying could be a criminal offence.

12.3 Cyberbullying may take the form of:

- sending rude, abusive, or threatening messages via email, text or social media
- posting insulting, derogatory, or defamatory statements on blogs or social networking sites
- setting up websites that specifically target the victim
- making and sharing derogatory or embarrassing videos of someone via mobile phone or email

12.4 Most incidents of cyberbullying will not necessarily reach significant harm thresholds and will probably be best dealt with the School's own Anti-bullying & Cyberbullying or Computer Usage policies with the co-operation of parents.

In terms of Cyberbullying, students are taught:

- not to disclose their password to anyone
- to only give out mobile phone numbers and email addresses to people they trust
- to only allow close friends whom they trust to have access to their social networking page
- not to respond to offensive messages
- to tell a responsible adult about any incidents immediately.

13.0 HANDLING E-SAFETY COMPLAINTS & CONCERNS

13.1 Complaints:

- Complaints of internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headmaster.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Students and parents are made aware of the complaints procedure.
- Students and parents will be informed of consequences and sanctions for students misusing the internet and this will be in line with the school's Behaviour Management Policy.
- All use of the school internet connection by community and other organisations is in accordance with the school e-safety policy.

13.2 Parents and carers are advised to be vigilant about possible cyberbullying and how to cut down on the risk of cyberbullying:

- Blocking any mobile numbers or social media accounts that are engaging in cyberbullying
- Internet service providers can trace messages being sent from a personal email account and can block further emails from the sender
- where bullying takes place in chat rooms, the child should leave the chat room immediately and seek advice from parents; bullying should be reported to any chat room moderator to take action
- website providers can remove comments from social networking sites and blogs and in extreme cases, can block the bully's access to the site
- the child could change mobile phone numbers or email addresses.
- the child should take a photo or screenshot of any abusive comments/messages posted on social media and report it to their tutor or Head of Year

14.0 INAPPROPRIATE CONTACTS AND NON-CONTACT SEXUAL ABUSE

14.1 Concerns may be raised about a child being at risk of sexual abuse as a consequence of their contact with an adult they have met over the internet. If reported to the School, students and parents are advised on how to terminate the contact and change contact details where necessary to ensure no further contact. Parents are advised to be vigilant of their child's internet use and report any concerns or incidents.

14.2 Children may also be sexually abused online through video messaging on Social Media Platforms. In these cases, perpetrators persuade the child concerned to carry out sexual acts while the perpetrator watches/records them. The perpetrators may be adults but may also be peers.

14.3 In the event of such an incident, the child should be taught how to use the CEOP "Report Abuse" button (displayed on the school website homepage) and parents should contact the police to report the incident.

14.4 Staff and parents should contact Surrey Children's Services on 0300 470 9100 (or if outside working hours, the emergency duty team on (01483) 517898 for advice on making a referral where there are concerns that the child:

- is being groomed for sexual abuse
- is planning or has arranged to meet with someone they have met on-line
- has already been involved in making or viewing abusive images
- has been the victim of non-contact sexual abuse.

14.5 If staff or parents are aware that a child is about to meet an adult they have made contact with on the internet, they should contact the police on 999 immediately.

15.0 ONLINE CHILD SEXUAL EXPLOITATION (CSE)

15.1 CSE describes situations where a young person takes part in sexual activity either under duress or in return for goods, food or accommodation. A key element of CSE is that there is a power imbalance in the relationship, for example often the perpetrator is much older than the child, who may not aware that they are being abused.

15.2 Staff should be aware that children can be sexually exploited online, for example posting explicit images of themselves in exchange for money or goods.

15.3 If staff are concerned that a child they work with is being sexually exploited online, they should inform the Designated Safeguarding Lead immediately, who may make a multi-agency referral.

16.0 CONTACT WITH VIOLENT EXTREMISTS

16.1 Many extremist groups such as far right groups, animal rights activists and fundamentalists who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

16.2 The Channel project is part of the government's Prevent strategy to divert young people away from extremism, and the Designated Safeguarding Leads in the Senior School and the Prep School have received training.

16.3 Staff need to be aware of those students who might be targeted by or exposed to harmful influences from violent extremists via the internet. Young people should be warned of the risks of becoming involved in such groups and it is against the school's rules to access such sites.

16.4 The School ensures that adequate filtering is in place, and reviews the filtering process whenever there is any incident of a student accessing websites that advocate violent extremism.

16.5 The e-Safety Co-ordinator (DSL) records and reviews all incidents in order to establish whether there are any patterns of extremist groups targeting the service and where relevant would contact the relevant agencies to report the situation.

16.6 If there is evidence that a young person is becoming deeply enmeshed in extremist narrative, staff would seek advice from Surrey's Youth Support Services on accessing programmes under the Channel project to prevent radicalisation.

16.7 Either contact Surrey via their email address: counter.extremism@education.gsi.gov.uk or call 020 7340 7264

17.0 WEBSITES ADVOCATING EXTREME OR DANGEROUS BEHAVIOURS

17.1 Some internet sites advocate dangerous activities such as self-harming, suicide, or anorexia. Other sites contain sexually explicit material or glorify risky and illegal behaviours like substance misuse.

17.2 Exposure to potentially harmful materials online may normalise the issue for young people and desensitise them to the harm. Most young people who visit these sites will not be adversely affected, but some vulnerable, less resilient young people may feel drawn to the sites which may trigger harmful or even fatal behaviours.

17.3 The Senior School can provide young people with an opportunity to discuss issues such as self-harming and suicide in an open manner and support any young person who is affected by these issues.

17.4 Staff should receive the training needed to raise awareness of these issues so that they are able to identify those young people who are at risk, offer appropriate support and make appropriate referrals for help.

17.5 Where staff are aware that a young person is accessing such websites and that this is putting them at risk of harm, they should consider making a referral to the relevant Children's Services (depending on which county the child lives in).

18.0 STAFF AND THE E-SAFETY POLICY

All Senior School staff are given Lingfield College's e-Safety Policy

- All staff will sign to acknowledge that they have read and understood the e-safety policy and agree to work within the agreed guidelines.
- Staff are made aware in the Staff Code of Conduct that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff who manage filtering systems or monitor ICT use are supervised by senior management and have clear procedures for reporting issues.

19.0 ENLISTING PARENTS' SUPPORT

19.1 Parents and carers have access to the e-Safety Policy on the school website.

19.2 The Senior School will ask all new parents to sign the parent /student agreement when they register their child with the school, and every existing student will be expected to read through the agreement with their tutors and click to agree to it via a Firefly task.

19.3 The school offers parents the chance to receive relevant e-Safety guidance by means of letters, events such as Tutor Evenings or by inviting external speakers in to talk to them.

20.0 OTHER POLICIES AND DOCUMENTS LINKED TO THIS E-SAFETY DOCUMENT

- Anti-bullying & Cyberbullying (LP-PW-003)
- Complaints (LP-MS-004)
- Computer Usage (LP-MW-012)
- Data Protection (LP-MW-014)
- Educational Visits (LP-CW-009)
- Exclusion (LP-MW-005)
- Safeguarding and Child Protection Policy (LP-PW-034)
- SEND (LP-CJ-022 & LP-PS-033)
- Staff Code of Conduct (LP-RW-008)
- Use of Digital Images (LP-PW-043)
- Whistleblowing (LP-MW-007)
- Digital Literacy and E Learning Policy (LP-CS-038)
- Mobile Phone Policy (LP-PW-039)
- Remote Learning Policy (LP-MW-049)

Last reviewed August 2023

Next review due August 2024