E-Safety (Prep School) Policy

Ref: ***LP-PP-012***	Version: ***6.1***	Date: *11th January 2024*
Document Owner: **Helen Roe *(ICT Subject Coordinator)***		
Description: This policy outlines the Prep 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 The school 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. It is essential that children are safeguarded from potentially harmful and inappropriate online material. Keeping Children Safe in Education 2021 gives guidance on the subject of online safety in schools:

1.2 **All** staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse their peers online, this can take the form of abusive, harassing, and misogynistic messages, the non-consensual sharing of indecent images, especially around chat groups, and the sharing of abusive images and pornography, to those who do not want to receive such content.' This Policy explains how we will protect and educate pupils and staff in their use of technology. This includes how we look to identify, intervene in, and escalate any concerns where appropriate.

1.3 E-safety can be described as the school's ability to:

- Protect and educate pupils and staff in their use of technology.

- Have the appropriate mechanisms to intervene and support any incident where appropriate.

1.4 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 pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group

(https://apwg.org/).(KCSiE 2021)

1.5 In order to help our pupils to better understand these areas of risk, the Prep School has adopted the acronym SMART. This stands for Safe, Meeting, Accepting, Reliable and Tell.

1.6 The e-Safety Policy is part of the School Development Plan and 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.

1.7 The Prep School's e-Safety Co-ordinator is the Head of Prep School, who is also the Designated Safeguarding Lead.

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

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 pupils, 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 It is recognised that keeping safe on-line is as much about educating pupils to think critically and about appropriate behaviour on-line as technical solutions. 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, coupled with poor social skills.

2.3 The below details our approach on the use of the internet in school:

- The internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

- Pupils 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 Computing & PSHE (SCARF) programme, assemblies every other year and often within the Drama curriculum in an age-appropriate way. This is addressed each year as pupils become more mature, and the nature of newer risks is identified. A staff e-safety guide with objectives and resources for each year group is kept in the computing folder in SharePoint Prep Staff Common under Internet Safety.
- The school SMART rules (detailed in the section below) are taught explicitly to all year groups. The e-safety curriculum underpins the e-safety SMART agreement that pupils and their parents/carers are required to sign at the start of each academic year
- Pupils are educated in the safe, effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils 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.
- The school uses 'Education for a Connected World' as a means of auditing its provision. The school also subscribes to 'National Online Safety' for information and resources which are used to keep parents up to date in risks on line through our weekly newsletter as well as provide resources for teachers to use in Computing lessons.
- Pupils and parents/carers in Years 5 and 6 are invited to attend Internet Safety Workshops biannually and then again in the Senior School.
- Pupils in Key Stage 2 are taught how to report unpleasant internet content to the teacher.
- The school's Acceptable Use of Computers Policy is given in full at the point of log-on for every student and member of staff.
- The school's internet access is provided by Zen Internet, which includes filtering appropriate to the age of pupils. However we are aware that this may not be the same for children at home and that education about how to stay safe is crucial.
- The school seeks to ensure that the use of internet-derived materials by staff and by pupils complies with copyright law.

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 then 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

3.0 SMART E-SAFETY RULES

3.1 Every year children and their parents/carers are required to sign an e-safety SMART agreement. This is linked to the SMART acronym (Safe, Meeting, Accepting, Reliable and Tell). During assemblies that take place bi-annually, this set of rules are delivered to all year groups at an age appropriate level. At the start of Year 1 and Year 3 they are taught explicitly and are reinforced and referred to in Computing lessons in all other year groups and are built upon as the maturity of the children develop.

3.2 The display in the main computing room shows the e-safety rules and agreements. These rules are also on display next to any computers in classrooms that children have access to. All computers accessed by the children have a 'Remember SMART' sticker attached to them.

Rules for KS1

S I will stay **SAFE** by not putting any of my details on the internet, like my phone number or address.

M I will not **MEET** anyone online I don't know in real life.

A I will not **ACCEPT** and open emails and messages from people I don't know.

R I understand that information I find on the internet may not be **RELIABLE** or true. I will check by asking an adult.

T I will **TELL** my teacher or parent if something online makes me feel uncomfortable or worried, or if someone I know is being bullied online. If I see something on screen that I am unhappy with I will turn off or minimise the screen and tell a teacher.

Rules for KS2

S I will stay **SAFE** by being careful not to give out personal information when chatting or posting online. Personal information includes your email address, phone number and password.

M **MEET**ing someone you have only been in touch with online can be dangerous. People I speak to online are still strangers even if I have been talking to them for a long time. I will not **MEET** anyone I don't know in real life.

A I will not **ACCEPT** and open emails, attachments or IM messages from people I don't know or trust. I know that these can contain viruses or nasty messages.

R I understand that information I find out on the internet may not be **RELIABLE** or true. I will check information by looking at other websites, in books, or with someone who knows. I also understand that someone I speak to over the internet may be lying about who they are.

T I will **TELL** my teacher or parent if something online makes me feel uncomfortable or worried, or if someone I know is being bullied online. If I see something on screen that I am unhappy with I will turn off or minimise the screen and tell a teacher.

3.3 Other rules: (applicable to both key stages)

- The messages I send will always be polite and sensible.

- I will only use the computers/iPADs with permission and as instructed by the teacher.
- I will keep my computer user name and password secret. My teacher will keep a list of my computer user name and password if I forget them.
- I will not upload photographs of myself and/or my friends which have been taken in school or whilst we are in school uniform onto social media sites.

3.4 Most situations we experience in the Prep School are encompassed under the rules above, however there are some more explicit statements which can be found in the School Behaviour Management Policy and School Rules and these rules form part of the e-safety agreement that children in KS2 sign. They are as follows:

- Pupils must not interfere with the work of others or the system itself.
- No one must create, store, transmit or cause to be transmitted material which is offensive, obscene, indecent or defamatory or which infringes the copyright of another person.
- Pupils must not gain or attempt to gain unauthorised access to other people's files or facilities or services accessible via local or national networks or transmit any confidential information about the School: they must not attempt to get around service limitations placed on network use by the School (or its agents).
- Pupils must not use school computers to access any social networking sites.
- Pupils must not under any circumstances use any social networking sites e.g Facebook or Twitter in order to bully or intimidate any pupil or member of staff or behave in any way online which could bring the school into disrepute.

4.0 SCHOOL SYSTEMS

4.1 The school system security is maintained and monitored daily by the ICT Engineers. The School uses Sophos and Senso to filter and monitor inappropriate content. 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. 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 pupils that has been blocked, and where relevant pupils and parents have been contacted to discuss the nature of such searches.

4.2 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.

MANAGING INTERNET ACCESS

5.0 PROCEDURES FOR DEVICE DATA SECURITY

5.1 Staff are responsible for the security of all data stored on their devices and must take appropriate measures to protect this data, this includes not leaving their devices unattended in public places, not sharing sensitive data with unauthorized parties, digitally locking the devices when not in use with a strong password/PIN and/or biometrics and ensuring that all photos and videos older than 1 week are not stored on the device unless there is a valid reason for retention as per GDPR regulations.

5.2 Staff should ensure all passwords are kept private and are not shared with others.

5.3 Devices are assigned on a per user basis. Staff are responsible for their own device and this device should not be given or swapped with another user without the consent of IT.

5.4 Any school accounts signed into the device should be secured with the same as the above, including the use of multifactor authentication where applicable.

6.0 WORKING OFF-SITE

6.1 The School provides each employee with OneDrive cloud storage. The School strongly recommends that the school data being worked on is accessed via these secure services when the use of a School managed device is not available.

6.2 If a USB and is used it is a requirement that it must be encrypted.

6.3 Devices should never be left unattended, and accounts should never be left signed in on unlocked devices when working off site.

7.0 DATA AND INFORMATION SECURITY

7.1 The use and storage of data and information is a critical component of the Bring Your Own Device policy and the use and sensitivity of data should be taken into extreme consideration. Only the authorised users should be able to view restricted data, and a conscience effort should be made to ensure that this is applied. If you are in any doubt as to whether data can be stored on your device, you are required to consult with your manager or seek advice from the IT Helpdesk.

7.2 You should ensure that only the authorised user is able to access data relating to the School. For example, if you are sharing a device, all School accounts and restricted data should be removed once you have finished using the device.

7.3 Passwords and accounts should not be shared, if you feel your password or account has been comprised, you should change contact IT support immediately.

7.4 Personal or sensitive data, as defined by the GDPR, should never be stored on personal devices, locally or on cloud services not managed by the School. Storage, such as the OneDrive and SharePoint cloud storage accounts provided to you by the School should be used instead.

7.5 Any School information stored on your device should be deleted once you have finished with it, including deleting copies of email attachments.

7.6 All School information must be removed from your device and return it to the manufacturers' settings before if it sold, exchanged, or disposed of.

8.0 SYSTEM AND DEVICE SECURITY

8.1 The College takes information and systems security very seriously and invests significant resources to protect data and information in its care. When you use your own device as a work tool, you must maintain the security of the School's information you handle. The use of your own device must adhere to the IT User Policies, namely the computer usage and Bring Your Own Device (BYOD) Policy as well as any UK laws relating to the use of IT devices.

8.2 It is your responsibility to familiarise yourself with the device sufficiently to keep data secure, including preventing the theft and loss of data, as well as maintaining the integrity and confidentiality of data and information.

8.3 You must:

- Use the device's security features, such as a Biometric, PIN, Password, and automatic lock to help protect the device when not in use.
- Enable multifactor authentication on any account that's applicable.
- Ensure devices and data is encrypted where possible.
- Keep the device software up to date, for example using Windows Update or Software Update services.
- Activate and use encryption services and anti-virus protection if your device features such services.
- Install and configure tracking and/or wiping services, such as Apple's 'Find My iPhone app', Androids 'Where's My Droid' or Windows 'Find My Phone', where the device has this feature. This is to enable you to locate or wipe your device should it go missing.
- Only use applications approved by the School to access school content. This includes but is not limited to Microsoft Edge, Microsoft OneDrive, Microsoft Outlook, Microsoft Office (including all apps in the suite). If you are unsure if an application is approved, please contact IT Support.
- Ensure your device is never left unattended when the device is unlocked and has access to the School's data.
- Never attempt to circumvent the device manufacturer's security mechanisms in any way, for example to 'jailbreak' the device.

9.0 AUTHORISING INTERNET ACCESS

9.1 All staff must read and sign the 'Staff Code of Conduct for ICT' before using any school ICT resource.

9.2 The school maintains a current record of all staff and pupils who are granted access to school ICT systems

9.3 Pupils apply for internet access individually by agreeing to comply with the Responsible Internet Use statement when they log on to any school computer or device.

10.0 ASSESSING RISKS

10.1 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.

10.2 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.

11.0 MANAGING FILTERING

11.1 If staff or pupils come across unsuitable on-line materials, the site must be reported to the Designated Safeguarding Leader (J. Shackel) and to ICT.

11.2 Staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Staff check any website they wish to use with pupils for appropriate content. This will be done before the lesson takes place.

12.0 MANAGING EMERGING TECHNOLOGIES

12.1 Emerging technologies will be examined for educational benefit.

12.2 Mobile phones and associated cameras are not be used during lessons or formal school time. Pupils are only allowed phones in school in exceptional circumstances and with permission from the Head of Prep School.

12.3 The appropriate use of Firefly, laptops and alternative learning platforms is discussed as the technology and resources become available within the school. Pupils from Years 1 to 6 may use Firefly and Teams, especially when remote learning. The Nursery use FAMLY as a Management Software System in which to track children's progress through formative and summative assessment.

12.4 Staff use of mobile devices is restricted during the school day when they are around pupils, and reference is made to this in both the Staff Code of Conduct and the Safe Working Practice forms. It is not permissible for any adults to use mobile phones in the EYFS. All personal mobile phones must be locked away upon entering the building.

12.5 Staff will use a school phone where contact with parents is required, unless necessary on school excursions or sporting fixtures.

13.0 PUBLISHED CONTENT AND THE SCHOOL WEBSITE

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

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

14.0 E-SAFETY TRAINING FOR STAFF

14.1 It is important that all staff are aware of the risks online activity poses to children. They must be aware that this risk includes the danger of children being exposed to extremist and terrorist material online. Prevent awareness training is being rolled out across the school.

14.2 The Designated Safeguarding Leader (DSL – J Shackel) will be responsible for keeping staff up to date via the following:

- Staff meetings, which provide a weekly forum for updates.
- Staff and pupils have annual training on e-safety.

- **Keeping Children Safe in Education** (statutory guidance for schools and colleges September 2023) will be distributed to all staff and there will be whole staff child protection inset days every three years and new staff will receive training on child protection within 3 months of starting or during induction.

15.0 CHILD USER ACCOUNTS

15.1 All children from years 1 – 6 are issued their own username and password for access to the school computers which are changed each year. They will also have a username and password for any learning platforms that they may use eg. Firefly, Microsoft Teams, Spelling Shed, Mathletics, Google apps. Children are taught the importance of keeping their log in details secret and not sharing them unnecessarily to help them develop good habits from an early age. KS1, Reception and nursery age children will use a class log in.

15.2 As from September 2022 children's work in Years 1-6 will (as far as reasonably possible) upload their work or add a link to their work to Seesaw (an online platform). Children are taught to respect each other's work and are not permitted to access other children's work without their permission. Teacher's feedback and pupil's evaluations will also be found on Seesaw.

15.3 Children in years 1-6 are currently able to save work to 'Junior Common' however, during Autumn 2023 this will change to a specific area on SharePoint in addition to their personal OneDrive account.

16.0 E-MAIL

16.1 Pupils in all Years are given a school email address. They are taught how to use email in a safe way including how to deal with junk mail and email from unauthorised senders.

When using email, students are taught:

- to keep messages polite.
- not to disclose personal contact details for themselves or others.
- to tell their parent, carer or teacher immediately if they receive an offensive or distressing email.
- not to use email to bully or harass others.
- to be wary of opening attachments to emails where they are unsure of the content or have no knowledge of the sender.

16.2 From KS2 suitable forms of email communication are regularly explained to pupils in accordance with the guidelines set out by the information and Records Management Society (www.irms.org.uk)

16.3 SMART posters are displayed in all rooms where computers are used.

16.4 Pupils must immediately tell a teacher if they receive an offensive e-mail or Teams message.

16.5 Pupils are advised not to reveal personal details about themselves or others in e-mail communication or Teams message, or arrange to meet anyone without specific permission.

16.6 Staff to pupil 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.

16.7 Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.

16.8 The forwarding of chain letters is not permitted.

17.0 USE OF CAMERAS, MOBILE PHONES, PUBLISHING CHILDREN'S DETAILS/PHOTOGRAPHS ONTO THE SCHOOL WEBSITE AND SOCIAL MEDIA

*See Use of Digital Images Policy (LP-PW-043) and Safeguarding and Child Protection Policy (LP-PW-034).

18.0 CYBERBULLYING

18.1 Cyberbullying is defined as the use of ICT 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.

18.2 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.

18.3 Cyberbullying may take the form of:

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

18.4 Most incidents of cyberbullying will not necessarily reach significant harm thresholds and will probably be best dealt with the service's own anti-bullying or acceptable use policies with the co-operation of parents.

18.5 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.

19.0 HANDLING E-SAFETY COMPLAINTS & CONCERNS

19.1 Complaints of internet misuse will be dealt with by a senior member of staff.

19.2 Any complaint about staff misuse must be referred to the Headmaster.

19.3 Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

19.4 Pupils and parents are made aware of the complaints procedure.

19.5 Pupils and parents will be informed of consequences and sanctions for pupils misusing the internet and breaking the SMART rules and this will be in line with the school's Behaviour Management Policy.

19.6 All use of the school internet connection by community and other organisations is in accordance with the school e-safety policy.

19.7 Parents and carers are advised to be vigilant about possible cyberbullying and how to work with internet and mobile service providers to cut down on the risk of cyberbullying:

- mobile phone companies can trace calls and ensure that any further calls and texts from that number are blocked
- 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.

20.0 INAPPROPRIATE CONTACTS AND NON-CONTACT SEXUAL ABUSE

20.1 Children may also be sexually abused online through video messaging such as Skype. 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.

20.2 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.

20.3 In the event of such an incident, the child should be taught how to use the CEOP "Report abuse" button (normally displayed on the screen) and parents should contact the police to report the incident.

20.4 Staff and parents should contact Surrey Children's Services through the Children's Single Point of Access (C-SPA) on (0300) 470 9100, e-mail **cspa@surreycc.gov.uk** (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
- is related to radicalisation or terrorism
- has already been involved in making or viewing abusive images or nude images
- has been the victim of non-contact sexual abuse.

20.5 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.

21.0 ONLINE CHILD SEXUAL EXPLOITATION (CSE)

21.1 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.

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

21.3 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.

22.0 WEBSITES ADVOCATING EXTREME OR DANGEROUS BEHAVIOURS

22.1 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.

22.2 Exposure to potentially harmful materials online (including anything related to radicalisation or terrorism) 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.

22.3 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.

22.4 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 Surrey Children's Services through the Children's Single Point of Access (C-SPA).

23.0 STAFF AND THE E-SAFETY POLICY

23.1 All staff are given the School e-Safety Policy and its importance explained.

- 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 in the Senior School and have clear procedures for reporting issues.

23.2 In cases where there is an online element such as sexting, specific advice must be followed:

- **Never** view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.
- If you have already viewed the imagery by accident (e.g. if a young person has showed it to you before you could ask them not to), report this to the DSL (or equivalent) and seek support.
- **Do not** delete the imagery or ask the young person to delete it.
- **Do not** ask the child/children or young person(s) who are involved in the incident to disclose information regarding the imagery. This is the responsibility of the DSL (or equivalent).
- **Do not** share information about the incident with other members of staff, the young person(s) it involves or their, or other, parents and/or carers.
- **Do not** say or do anything to blame or shame any young people involved.
- **Do** explain to them that you need to report it and reassure them that they will receive support and help from the DSL (or equivalent).

24.0 ENLISTING PARENTS' SUPPORT

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

24.2 The school will ask all new parents to sign the SMART agreement when they register their child with the school, and every existing pupil will be expected to sign the agreement every year.

24.3 The school is looking into ways in which parents can be given e-safety training with a focus on education and being given an overview of the means by which they can take control whilst not undermining trust.

24.4 Often children do not wish to be constantly online but often lack sufficient alternatives for play, travel, interaction and exploration. Parents should be encouraged, where appropriate, to interact with their children on the internet as well as provide other opportunities for recreation.

24.5 Homework tasks may be uploaded to Firefly, therefore parents may wish to check this to see status.

25.0 OTHER POLICIES AND DOCUMENTS LINKED TO THIS E-SAFETY POLICY:

25.1 Policies

- Anti-bullying Policy & Cyberbullying (LP-PW-003)
- Behaviour Management Policy (LP-PP-005 Prep and LP-PS-006 Senior)
- Complaints Policy (LP-MW-023)
- Safeguarding and Child Protection Policy (LP-PW-034)
- Staff Code of Conduct (LP-RW-008)
- Data Protection Policy (LP-MW-014)
- Use of Digital Images (LP-PW-043)
- Whistleblowing (LP-MW-007)
- Exclusion Policy (LP-MW-005)
- Inclusion and SEND (LP-CP-022 Prep and LP-PS-033 Senior)
- Internet and Social Networking Policy (Staff)
- Computer Usage Policy (LP-MW-012)
- See School Rules

25.2 Documents

- The Data Protection Act (2018) and GDPR UK
- The Computer Misuse Act (1990)
  - Unauthorised access (e.g. using another user's username and password)
  - "hacking", "introduction of viruses"
  - Unauthorised modification of the contents of a computer (installing software in your account)
- The Copyright, Designs and Patents Act (1988)
- Copyright (computer programs) regulations (1992)

  It is an offence to:
  - Copy software unless allowed by license
  - Download copyright materials (which may include MP3's)
  - Link to a site that contains material used without permission
- Public Interest Disclosure Act (1998)
- Obscene Publications Act (1959)
  - It is an offence to sell, hire or lend material that is obscene
  - This includes publishing or downloading pornographic or other offensive material from the web

- Telecommunications Act (1984)
  - It is an offence to transmit messages over telecommunications systems (including computer networks) of an obscene, slanderous, threatening or annoying nature
  - This INCLUDES the contents of e-mail
- Theft Act (1968)

  The following acts are ILLEGAL:
  - Hacking
  - Intentional introduction of viruses
  - Giving someone unauthorised access (which includes giving away your password): It is NOT your account to lend to others. Actions of another whilst using your account are YOUR responsibility.
  - Downloading/storing material that is obscene
  - Downloading illegal copies of software
  - Sending messages of an obscene, slanderous, threatening nature
  - Installation of unlicensed software

25.3 These explanations are intended to be a guide as to how the acts relate to your use of the computing or network facilities and are not a legal interpretation of those acts.

26.0 DISCIPLINARY ACTIONS

Depending on the severity of the offence, either one or two or all of the following actions taken could be:

- Informal Warning given in school.
- Letter sent home (recorded in pupil's file).
- Withdrawal of ALL parts of user account.

27.0 DAMAGE TO EQUIPMENT:

The following Damage to Equipment policy statement will be published:

- Any purposeful or wilful damage (be this at a physical or software level) to or theft of equipment will be charged for at the current rate. Theft of equipment of any kind takes money away from that available to improve facilities within the school.
- It is in your own interest, and the interest of other pupils within the school, that the computer equipment is treated with utmost respect.
- Damage to or theft of equipment will cause inconvenience to you and to others.

Next review due August 2024