E-Safety Policy

Including all of the Pre-Prep Department and Early Years Foundation Stage

CWL / TS

September 2022

Review and Amendment Record

Date	Person Conducting the Review	Changes Made
Sep 2021	DJJK, TS, DRW, JERA	New Policy
Sep 2022	DJCF, CWL	Annual review for induction; new policy holder

Legal Requirements & Education Standards

References:
A: Commentary on the Regulatory Requirements September 2021, Part 3 (www.isi.net)
B: Reference Guide to the key standards in each type of social care service inspected by Ofsted (www.ofsted.gov.uk)
C: Health and Safety at Work" Section H of the ISBA Model Staff Handbook
D: "Health and Safety and Welfare at Work" Chapter N of the ISBA Bursar's Guide
E: "Insurance" Chapter K of the Bursar's Guide by HSBC Insurance Brokers Ltd
F: UK Council for Child Internet Safety (www.edcuation.gov.uk/ukccis)
G: Cyber-bullying.org (www.cyberbullying.org)
H: Department for Education "Safer Working Practice for Adults who Work with Children and Young People" (www.education.gov.uk)
I: DfE Data Protection: a toolkit for schools

Circulation for comment and input:

Headmaster, Deputy Headmaster, Operations Director, Designated Safeguarding Lead, Deputy Head Pastoral, IT Network Manager.

Publication:

School website and school policy folder

INTRODUCTION

It is the duty of Summer Fields to ensure that every pupil in its care is safe; the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning, in addition to traditional methods, but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Current and emerging technologies used in and outside of school include:

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

This policy, supported by the Acceptable Use Policy (for all staff, visitors and pupils), is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It should be read in conjunction with the school's Safeguarding Policy, Staff Code of Conduct, Acceptable Use Policies and Behaviour Policy.

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

At Summer Fields, we understand the responsibility to educate our pupils on e-Safety issues, teaching them the appropriate behaviours and critical-thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about e-Safety and listening to their fears and anxieties as well as their thoughts and ideas.

SCOPE OF THIS POLICY

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

Both this policy and the Acceptable Use Policy (for all staff, visitors and pupils) cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, goose-necked cameras, webcams, tablets, whiteboards, digital video equipment, etc.); also all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.)

ROLES AND RESPONSIBILITIES

1. The Governing Body

The governing body of the school is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually via the Compliance Committee, chaired by the compliance governor.

2. Headmaster and the Senior Management Team

The Headmaster is responsible for the safety of the members of the school community and this includes responsibility for e-Safety. The Headmaster has delegated day-to-day responsibility to the Deputy Head, Pastoral as the e-Safety coordinator. The Deputy Head, Pastoral works closely with the Deputy Headmaster and the Head of Pre-prep on e-Safety.

In particular, the role of the Headmaster and the Senior Leadership team is to ensure that:

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

3. E-Safety coordinator

The school's e-Safety coordinator is responsible to the Headmaster for all 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 the IT Network Manager 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 Oxfordshire Safeguarding Children Board. The e-Safety coordinator will:

(a) compile and keep logs of e-Safety incidents
(b) report to the Headmaster on recorded incidents
(c) ensure that staff are aware of this guidance
(d) provide / arrange for staff training
(e) liaise with It Network Manager
(f) liaise with the Headmaster, Deputy Headmaster and Head of Pre-prep (as appropriate) on any investigation and action in relation to e-incidents, and
(g) advise on e-Safety policy review and development.

4. IT Network Manager

The IT Network Manager has a key role in maintaining a safe and secure 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 e-Safety coordinator. The IT Network Manager will:

(a) be responsible for the IT infrastructure and that it is not open to misuse or malicious attack.
(b) ensure that users may only access the networks and devices through an enforced password protection policy.
(c) keep up to date with e-safety technical information in order to carry out their role.
(d) ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse, and
(e) implement any agreed monitoring software / systems.

5. Teaching and support staff

All staff are required to sign the Staff Acceptable Use Policy before accessing the school's systems. As with all issues of safety at the 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. Teaching and support staff are to:

(a) maintain awareness of school e-Safety policies and practices.
(b) report any suspected misuse or problem to the Headmaster or E-Safety Co-ordinator.
(c) ensure that all digital communications with pupils / parents / carers / fellow staff are on a professional level and conducted on school systems.
(d) where relevant e-Safety is recognised in teaching activities and curriculum delivery.
(e) ensure pupils understand and follow e-Safety policies, including the need to avoid plagiarism and uphold copyright regulations.
(f) monitor the use of digital technologies (including mobile devices, cameras, etc. during school activities, and
(g) ensure that where the use of the internet is pre planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

6. Pupils

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

(a) are responsible for using school digital technology systems in accordance with the school Acceptable Use Policy.
(b) will understand and follow e-Safety policies, including the need to avoid plagiarism and uphold copyright regulations.
(c) will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.
(d) are expected to understand policies on the use of mobile devices and digital cameras, the taking and using of images, and cyber-bullying, and
(e) will understand that the E-Safety Policy will include actions outside of school where related to school activities.

7. Parents and carers

Summer Fields believes that it is essential for parents to be fully involved with promoting e-Safety both in and outside of school. We regularly consult and discuss e-Safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. We do this by way of letters, in the weekly newsletter, and on the school's remote learning portal.

The school adopts a collaborative approach with parents and carers to develop both the understanding and habits associated with appropriate and healthy on-line behaviour. Parents and carers are provided with resources to support their children and opportunities are provided to meet and discuss issues with experts in the field of E-safety.

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

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

(a) will be advised of e-Safety policies through parents' evenings, newsletters, letters and the school website.

(b) will be encouraged to support the school in the promotion of good e-Safety practice; and,

(c) should follow school guidelines on:

(i) digital and video images taken at school events

(ii) access to parents' sections of the school website and pupil records; and

(iii) their children's personal devices in the school (where this is permitted).

8. Community Users / Contractors

Where such groups have access to school networks or devices, they will be expected to provide signed acceptance to abide by school e-Safety policies and procedures.

EDUCATION AND TRAINING

1. Staff: awareness and training

New staff receive information about Summer Fields's E-Safety and Acceptable Use Policies as part of their induction.

All staff receive regular information and training on e-Safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety. All supply staff receive information about e-Safety as part of their safeguarding briefing on arrival at school.

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

Teaching staff are encouraged to incorporate e-Safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community. A record of concern must be completed by staff as soon as possible if any incident relating to e-Safety occurs and be provided directly to the school's e-Safety Coordinator and Designated Safeguarding Lead.

2. Pupils: e-Safety in the curriculum

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

The school provides opportunities to teach about e-Safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out in PSHE lessons, during presentations in assemblies and informally when opportunities arise.

At age-appropriate levels, and usually via the RSE provision, the PSHE curriculum and ICT lessons, pupils are taught about their e-Safety responsibilities and to look after their own online safety. From Reception, pupils have a dedicated computing lesson in the Pre-prep library/ICT suite. Their lessons cover areas including online safety and cyberbullying, the use of email and safe emails, and online searches. From year 4, pupils are taught about recognising online sexual exploitation, stalking and grooming and the risks involved, and of their duty to report any such instances they or their peers encounter. Pupils can report concerns to the Designated Safeguarding Lead, the E-Safety Coordinator or any member of staff at the school.

From year 7, pupils are also taught about relevant laws applicable to using the internet, such as data protection and intellectual property. Pupils are taught about respecting other people's information and images through discussion and classroom activities.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Countering Bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach Designated Safeguarding Lead, e-Safety Coordinator or School Counsellor - as well as parents, peers and other school staff - for advice or help if they experience problems when using the internet and related technologies. Pupils are regularly provided with resources to help guide their on-line behaviour. They are also provided with the opportunity to meet and discuss issues relating to e-Safety with experts in the field.

3. Parents

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

The school recognises that not all parents and guardians may feel equipped to protect their son when they use electronic equipment at home. The school therefore arranges events for parents when an outside specialist advises about e-Safety and the practical steps that parents can take to minimise the potential dangers to their sons without curbing their natural enthusiasm and curiosity. Further resources are supplied to help parents regularly throughout the year.

POLICY STATEMENTS

1. Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device, staff should ensure that it is locked to prevent unauthorised access. Devices issued to staff are encrypted, to protect data stored on them.

Staff at Summer Fields are permitted to bring in personal devices for their own use. They may use such devices in areas away from pupils.

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

Pupils

Boarders must leave all personal portable devices in their respective lodges under the care of their lodge parents between return to lodge at the start of term or after a Short Leave, Long Leave or Weekend Leave away from school; they will receive the device back when they next depart from school.

If day boys are given authorisation to bring a mobile phone to school (for instance for use during the journey to and from school), they should be left in the care of the School Secretary in Reception for the duration of the school day. Any device that communicates over the internet, including smartwatches and other wearable technology, are not permitted.

No personal devices belonging to pupils are to be used during lessons at school, whether for schoolwork or personal use.

School-owned mobile technologies that are available for pupil use, including laptops, tablets and cameras, are kept stored in lockable cabinets. Access is available via teaching staff. Members of staff should sign devices out and in before and after each use by a pupil.

The school recognises that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes – for instance monitoring the operation of a pump regulating the blood sugar levels of a boy who is diabetic – the pupil's parents or carers should arrange a meeting with the Head Sister, Head of Learning Support, Deputy Head, Pastoral, Head of Pre-prep or Deputy Headmaster (as appropriate). At this meeting it will be agreed as to how the school can appropriately support the use of mobile technology for the pupil's needs. The appropriate member of staff co-ordinating the school's support of the pupil in question will inform their teachers and other relevant members of staff about how the pupil will use the device at school.

2. Use of internet and email

Staff

Staff must not access social networking sites, or any website or personal email which is unconnected with school business, from school devices or while teaching or in front of pupils. Such access may only be made from staff members' own devices whilst in areas away from pupils.

When accessed from staff members' own devices or away from school premises, staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position and the reputation of the school.

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

Staff must immediately report to the IT Network Manager the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication. The IT Network Manager will liaise with the school's senior leadership if the communication has originated from another member of staff. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to the IT Network Manager.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm
- bring Summer Fields into disrepute
- breach confidentiality
- breach copyright
- breach data protection legislation, or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief, or age.
    - using social media to bully another individual, or
    - posting links to or endorsing material which is discriminatory or offensive.

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

Any digital communication between staff and pupils or parents / carers must be professional in tone and content. Under no circumstances may staff contact a pupil or parent / carer using a

personal email address. The school ensures that staff have access to their work email address when offsite, for use as necessary on school business.

Pupils

All pupils from Year 4 upwards are issued with their own personal school email addresses for use on the school network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure, and must be used for all schoolwork, assignments, research and projects. Pupils should be aware that email communications through the school network and school email addresses are monitored. In the Pre-prep, specific computing programmes are used to teach about the use of email.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for school work or research purposes, pupils should contact the IT Network Manager for assistance.

Pupils 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 IT Network Manager, e-Safety Coordinator, Designated Safeguarding Lead or another member of staff.

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

Pupils must report any accidental access to materials of a violent or sexual nature directly to the IT Network Manager, e-Safety Coordinator, Designated Safeguarding Lead or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the school's Behaviour Policy. Pupils should be aware that all internet usage via the school's systems and its Wi-Fi network is monitored.

3. Data storage and processing

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

Staff and pupils are expected to save all data relating to their work to their school laptop or PC, or to the school's central server or One Drive account.

Staff devices should be encrypted if any data or passwords are stored on them. The school does not allow any removable media (USB memory sticks, CDs, portable drives) to be used on the school site.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. No personal data of staff or pupils should be stored on personal devices.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Data Protection Lead, who is the school’s Operations Director .

4. Password security

Pupils in the prep school and staff have individual school network logins, email addresses and storage folders on the server. In the Pre-prep, pupils have a class login and their work is then stored in individual folders. They also have individual logins for any subscription services that the school subscribes to.

Staff and pupils are regularly reminded of the need for password security.

All pupils and members of staff should:

- use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which should be changed every six months.
- not write passwords down, and
- not share passwords with other pupils or staff.

5. Safe use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for 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 pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet, for instance on social networking sites.

Parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published on blogs or social networking sites without the permission of the people identifiable in them (or the permission of their parents), nor should parents comment on any activities involving other pupils in the digital or video images.

Staff and volunteers are allowed to take digital or video images to support educational aims but must follow this policy and the Acceptable Use 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.

The school's Safeguarding Policy makes clear the policy in the EYFS. In the EYFS setting mobile telephones must be locked away in the staff room. Only school cameras, iPads or other school devices may be used to take photographs, which must be promptly downloaded to the school computer system and then deleted from the device.

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

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

Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. See the Parent Contract and school Acceptable Use Policy for more information.

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

6. Monitoring

The school subscribes to a safeguarding and e-Safety monitoring system which monitors key strokes on all school devices and the school network, including both pupils and staff. Any concerns are reported by the monitoring company to the Headmaster (in the case of staff or a serious issue with a pupil)) or to the DSL, Deputy Head Pastoral and Head of eLearning (for the

majority of issues involving pupils) via an email report; a weekly report is also provided to help assess any key themes.

Any usage that poses a risk of immediate danger to an individual results in a phone call alert from the monitoring company to the Headmaster or DSL, or if they cannot be contacted, the Deputy Headmaster or Deputy Head Pastoral.

7. Misuse

Summer Fields will not tolerate illegal activities or activities that are inappropriate in a school setting, and will report illegal activity to the police and/or the Local Authority Designated Officer for safeguarding (LADO) for Oxfordshire. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the CEOP.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (in particular the Safeguarding Policy).

The school will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our Countering Bullying Policy.

Incidents of or concerns around e-Safety will be recorded and reported to the school's e-Safety Co-ordinator and the Designated Safeguarding Lead in accordance with the school's Safeguarding Policy.