Elstree School

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

E-Safety Policy

Contents

Person responsible for Policy: RMS/SCA
Date of last revision: July 2017
Date to be revised: August 2018

1. Introduction

It is the duty of Elstree school to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. ICT and online communication 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.

This is a whole school policy including EYFS.

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 guidelines on how to minimise risks and how to deal with any infringements. It is linked to the following policies:
Safeguarding policy;
Code of conduct;
Promoting positive behaviour policy;
Anti Bullying;
Acceptable Use Policy for ICT;
Data Protection Policy;
PSHEE Policy;
ICT Policy (including Social Media).

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

At Elstree 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.

2. Scope of this policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors, who have access to and are users of the school ICT 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 ICT cover fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils, staff, or visitors and brought onto school premises (personal laptops, tablets, smart phones, etc.).

3. Roles and Responsibilities

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 regularly.

The governor responsible for reviewing this policy is the Safeguarding Governor, **Emma McGrath.**

The 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 Headmaster and Head of ICT.

In particular, the role of the Headmaster and Senior Management Team is to ensure that:

Staff, in particular the Head of ICT, are adequately trained about e-safety; and staff are aware of the schools procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection with the school.

The Head of ICT (and E-Safety lead)

The Head of ICT has a key role in maintaining a safe technical infrastructure at the school and keeping abreast of the rapid succession of technical developments. He is 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 ICT. He monitors the use of the internet and emails, maintains content filters, and will report inappropriate usage to the Deputy Head or SMT.

Teaching and Support Staff

All staff are required to read the acceptable Use Policy for ICT before accessing the School's systems.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any e-safety issues which may arise in classrooms on a daily basis.

In the event of an issue relating to e-safety they need to notify the Head of ICT or Deputy Head.

Pupils

Pupils are responsible for using the School ICT systems in accordance with the Acceptable Use Policy for ICT, and for letting staff know if they see the ICT systems being misused.

Parents and Carers

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

Parents and carers are responsible for using the school ICT systems in accordance with the Acceptable Use Policy for ICT, and for letting staff know if they see ICT systems being misused.

4. Education and Training

Staff: Awareness and training

New staff receive information on the School's e-safety and Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training 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 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 for ICT.

Teaching Staff are encouraged to incorporate e-safety activities and awareness within their subject areas 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 Deputy Head or Head of ICT. If both are unavailable then a copy must be given to a member of the SMT.

Pupils: E-safety in the curriculum

ICT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be 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 safety within a range of curriculum areas and ICT lessons. Educating pupils on the dangers of technologies that may be encountered

outside school will be carried out via PSHEE, by presentation in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, via PSHEE and ICT, pupils are taught about e-safety responsibilities and to look after their own online safety. From Year 6, pupils are formally taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the Designated Safeguarding Lead and any member of staff at School.

From Year 5, 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 (etc.) through discussion and classroom activities in PSHEE lessons.

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 Anti Bullying Policy, which describes the preventative measures and the procedures that will be followed when the School discovers cases of bullying). Pupils should approach the Designated Safeguarding Lead, School Counsellor or a member of the SMT as well as parents, peers and other School staff for advice or help if they experience problems when using the internet and related technologies.

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 may feel equipped to protect their son or daughter when they use electronic equipment at home. The school therefore arranges regular discussion 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 and daughters without curbing their natural curiosity and enthusiasm.

The school will highlight and alert parents to e-safety concerns as they arise throughout the school year.

5. Policy Statements

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.

Staff (at Elstree) are permitted to bring in personal devices for their own use. They may use such devices in staff-only areas of the school during free lessons, break times and lunchtimes or in the classrooms so long as children are not around. In an emergency mobiles phones may be used in front of pupils to contact appropriate services.

They must not be used upstairs to the dormitories, changing rooms or toilets.

Staff, visitors, volunteers and students **(within the Early Years Foundation Stage, EYFS)** are not permitted to use their own mobile devices to take or record any images of Elstree children for their own records during session times.

Only school cameras and video equipment is used to record children in the Early Years. No photographs or videos are allowed to be taken on staff mobile phones. Photographs and recordings of children are only taken for valid reasons, i.e. to record their learning and development, or for displays within the setting. Children have their photographs taken on school cameras and downloaded onto the school system to provide evidence of their achievements for developmental records **(The Early Years Foundation Stage, EYFS).**

This applies to our EYFS and after school care.

Pupils

If pupils (full boarders only) bring in mobile phones and devices they must be handed into the Heads of Boarding at the start of term, end of exeats and half terms for safekeeping. Full boarders will have access to their devices in public areas (common rooms and library) on Wednesday evenings and at the weekends under supervision by the resident boarding staff. **They must not be used upstairs to the dormitories, changing rooms or toilets.**

School mobile technologies available for pupils including laptops, tablets, cameras, etc. are stored in the ICT office. Access is available via the Head of ICT. Members of staff should book devices in and out 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, the pupil's parents should arrange a meeting with the Head of Learning Support to agree how the school can appropriately support such use. The Head of Learning Support will then inform the pupils' teachers and other relevant members of staff about how the pupil will use the device at school.

School Trips

If pupils are able to bring in personal electronic devices for travelling to and from residential trips (e.g. Year 7 French Trip, Leavers' Trip, Rugby Tour, etc.), as agreed in the trip instructions to parents, these must be collected in each evening by the responsible staff to ensure pupils' safety. They should not be able to access wifi in residential centres, etc.

Use of Internet and Email
Staff

Staff must not access social networking sites or any website or personal email which is unconnected with school work or business from school from school devices or whilst teaching. Such access may only be made whilst in staff-only areas of school or classrooms so long as pupils are not present.

When accessing from staff members' own devices/ off 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 emails addresses are monitored.

Staff must immediately report to an appropriate member of the SMT of they receive any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening, or bullying in nature and must not respond to any such communication. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect of being fraudulent to the Head of ICT.
Any online communication must not either knowingly or recklessly;
Place a child or young person at risk of harm, or cause actual harm;
Bring the school into disrepute;
Breach confidentiality;
Breach copyright;
Breach date protection legislation; or do anything that could be considered discriminatory against, or bullying or harassment of, any individual, fr example by:

- Making offensive or derogatory comments relating to sex, gender reassignment, race, 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 be added as social network 'friends' or contacted through social media.

Any digital communication between staff and pupils or parents must be professional in tone and content. Only in exceptional circumstances, agreed by the Deputy Head, may staff contact a pupil or parent using any 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

Access is via a personal logon, which is password protected. This official email service may be regarded as safe and secure, and must be used for School work. Pupils should be aware that email communication through the school network and School email addresses are monitored.

There is a 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 purposes, pupils should contact the ICT support team for assistance.

Pupils should not respond to any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in tone and should report immediately such a communication to the ICT support Team.

The school expects pupils to think carefully before they post any information online, or re-post 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 material of a violent or sexual nature directly to the Head of ICT or another member of staff. Deliberate access to any inappropriate materials by pupils will lead to an incident being recorded on their file and will be dealt with under the school's behaviour management policy. Pupils should be aware that all internet usage via the school's systems and its wifi is monitored.

Certain websites are automatically blocked by the school's filterning system. If this causes problems for school work /research purposes, pupils should contact the Head of ICT for assistance.

Data Storage and Processing

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

Staff and pupils are expected to save all data relating to their work to their School PC or to the school's central server.

Staff devices should be encrypted if any data or passwords are stored on them. The School expects all removable media (USB memory sticks, CDs, portable drives) taken outside school or sent by post or courier to be encrypted before sending.
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 memory sticks, but instead stored on an encrypted memory stick provided by the school.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the Head of ICT or a member of the SMT.

Password Security

Pupils and staff have individual School network logons, email addresses and storage folders on the server. Staff and pupils are regularly reminded of the need for password security.

All pupils and staff should:

Use a strong password (usually containing eight characters or more, and containing upper and lower case letters as well as numbers), which they should change every 4 months;
Not write passwords down; and
Not share passwords with other pupils and staff.

Safe use of digital and video images

The development of digital imagines 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 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 any 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 risk 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 (e.g. on social networking sites).

Parents 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 case protection, these images should not be published on blogs or social networking sites (etc.) 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 / video images.

Staff and volunteers are allowed to take digital/video images to support education aims, but must follow this policy and the Acceptable Use Policy for ICT concerning the sharing, distribution and publication of these images. Those images should be taken on school equipment. Staff may use their phones/personal devices to take photos of school events on the strict understanding that these are downloaded onto the school system (within 24 hours) and deleted off their personal devices.

Care should be taken when taking digital /video images that pupils are appropriately dressed and 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 acceptable Use Policy for ICT for more information).

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

Misuse

The school will not tolerate illegal activities or activities that are inappropriate in a School context and will report illegal activity to the police and/ or the local safeguarding authority.
If the school discovered that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP.
Incidents of misuse or suspected misuse must be dealt with by staff in accordance with the school's policies and procedures (See Safeguarding and Promoting Positive Behaviour policies).

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 anti-bullying Policy.

6. Complaints

As with all issues of safety at Elstree, if a member of staff, a pupil or a parent has a complaint or concern relating to e-safety, prompt action will be taken to deal with it. Complaints should be addressed to the Head of ICT (e-safety Lead) or Deputy Head in the first instance, who will liaise with the SMT and undertake an investigation where appropriate. Please see the Complaint policy for further information.

Incidents or concerns around safety will be recorded and reported to the school's Designated Safeguarding Lead, in accordance with the School's Safeguarding Policy.