EATON SQUARE
SENIOR SCHOOL

E-Safety Policy & Acceptable Use Policy for Parents, Pupils ,Visitors and Staff

E-Safety Policy

Introduction

It is the duty of Eaton Square Senior (the 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. IT and online communications provide 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.
- Communication and Collaboration platforms

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 is linked to the following school policies:

- Safeguarding;
- Staff Behaviour;
- Health and Safety;
- Promoting good behaviour
- Anti-Bullying;
- Social Media;
- Data Protection; and
- PSHE.

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

At Eaton Square Senior School, 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 school 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, central team 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 enabled 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.).

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.

2. Head and the Senior Leadership Team
The Head is responsible for the safety of the members of the school community and this includes responsibility for e-safety.
In particular, the role of the Head and the Senior Leadership Team is to ensure that:

- staff are adequately trained about e-safety; and
- 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. IT staff
The School does not employ any technical staff but outsources the management of its IT systems to a third party. The technical staff at the third party have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system and its data. They are responsible for basic training of 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 Director of Operations (Schools).

4. Teaching and support staff
All staff are required to sign the 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.

5. 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.

6. Parents and carers

The 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 that parents will feel able to share any concerns with the school.

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

Education and training

1. Staff: awareness and training

New staff receive information on Eaton Square Senior School'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 Designated Safeguarding Lead.

2. Pupils: E-Safety in the curriculum

IT 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 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 via Wellbeing lessons, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, and usually via Wellbeing pupils are taught about their e-safety responsibilities and to look after their own online safety. Pupils are 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 the school. 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 classroom activities and Wellbeing classes.

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 as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

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 or daughter when they use electronic equipment at home. The school therefore arranges discussion evenings 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 enthusiasm and curiosity.

4. Use of internet and email

Staff

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

When accessed 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 email addresses are monitored.

Staff must immediately report to IT support 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. Staff must remain alert to the risk of fraudulent emails and should report emails they suspect to be fraudulent to IT support team.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm, or cause actual harm;
- bring Eaton Square Senior 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 (e.g. "liking") 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. 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 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

There is strong anti-virus and firewall protection on the School network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork/research purposes, pupils should contact their class/form teacher 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 a member of staff.

The school expects pupils to think carefully before they post any information online or repost or endorse ("like") 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 a 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.

Certain websites are automatically blocked by the school's filtering system. If this causes problems for schoolwork / research purposes, pupils should contact their class teacher for assistance.

The use of mobile phones in the classroom is limited to as an when a teacher believes it is appropriate, meaningful and purposeful for a learning outcome, such as to involve pupils in low stakes testing. Phones must be off at all other times.

5. Data storage and processing

The school takes its compliance with the GDPR seriously. Please refer to the Acceptable Use Policy for further details.

6. Password security

Pupils and staff have individual school network logins, Microsoft Office accounts and storage folders on the server. 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 6 months;
- not write passwords down; and
- not share passwords with other pupils or staff.

7. Misuse

Eaton Square Senior 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 LSCB. 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 Anti-Bullying Policy.

Complaints

As with all issues of safety at Eaton Square Senior School, if a member of staff, a pupil or a parent/carer has a complaint or concern relating to e-safety prompt action will be taken to deal with it. Complaints should be addressed in writing to the Head in the first instance, who will undertake an investigation where appropriate. Please see the Complaints Policy for further information.

Incidents of or concerns around e-safety will be recorded using a Concern form and reported to the Designated Safeguarding Lead in accordance with the school's Child Protection Policy.

IT Acceptable Use Policy

Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents, and visitors. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers (but access to systems is not intended in any way to imply an employment relationship). 'Parents' include, where applicable, pupils' carers and those with parental responsibility. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Online behaviour

As a member of the school community you should follow these principles in all of your online activities:

- Ensure that your online communications, and any content you share online, are respectful of others and composed in a way you would wish to stand by.
- Do not access, create or share content that is illegal, deceptive, or likely to offend other members of the school community (for example, content that is obscene, or promotes violence, discrimination, or extremism, or raises safeguarding issues).
- Respect the privacy of others. Do not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without going through official channels and obtaining permission.
- Do not access or share material that infringes copyright, and do not claim the work of others as your own.
- Do not use the internet to distribute malicious software, to damage, interfere with, or gain unauthorised access to the computer systems of others, or carry out illegal activities.
- Staff should not use their personal email, or social media accounts to contact pupils or parents, and pupils and parents should not attempt to discover or contact the personal email addresses or social media accounts of staff.

Using the school's IT systems and cloud-based subscriptions

Whenever you use the school's IT systems (including by connecting your own device to the network) or cloud-based subscriptions such as Office 365, you should follow these principles:

- Only access systems and software using your own username and password. Do not share your username or password with anyone else.
- Do not attempt to circumvent the content filters or other security measures installed on the school's IT systems, and do not attempt to access parts of the system that you do not have permission to access.
- Do not attempt to install software on, or otherwise alter, school IT systems.
- Do not use the school's IT systems in a way that breaches the principles of online behaviour set out above.
- Remember that the school monitors use of the school's IT systems, and that the school can view content accessed or sent via its systems.

Passwords

Passwords protect the School's network and computer system and are your responsibility. They should not be obvious (for example "password", 123456, a family name or birthdays), and nor should they be the same as your widely-used personal passwords. You should not let anyone else know your password, nor keep a list of passwords where they may be accessed and must change it immediately if it appears to be compromised. You should not attempt to gain unauthorised access to anyone else's computer or to confidential information to which you do not have access rights.

Use of Property

Any property belonging to the School should be treated with respect and care and used only in accordance with any training and policies provided. You must report any faults or breakages without delay.

Use of school systems

The provision of school email accounts, Wi-Fi and internet access is for official school business, administration and education. Staff and pupils should keep their personal, family and social lives separate from their school IT use and limit as far as possible any personal use of these accounts. Again, please be aware of the school's right to monitor and access web history and email use.

Monitoring and access

Staff, parents and pupils should be aware that school email and internet usage (including through school Wi-Fi) will be monitored for safeguarding, conduct and performance purposes, and both web history and school email accounts may be accessed by the school where necessary for a lawful purpose – including serious conduct or welfare concerns, extremism and the protection of others.

Any personal devices used by pupils, whether such use is permitted, may be confiscated and examined under such circumstances. The school may require staff to conduct searches of their personal accounts or devices if they were used for school business in contravention of this policy.

Compliance with related school policies

You will ensure that you comply with the school's e-Safety Policy, Retention of Records, Safeguarding, Anti-Bullying and Acceptable Use Policy.

Retention of digital data

Staff and pupils must be aware that all emails sent or received on school systems will be kept in archive whether or not deleted and email accounts will be closed, and the contents deleted within 1 year of that person leaving the school. Important information that is necessary to be kept should be held on the relevant personnel or pupil file, not kept in personal folders, archives or inboxes. Hence it is the responsibility of each account user to ensure that important information or indeed any personal information that they wish to keep, in line with school policy on personal use is retained in the right place or, where applicable, provided to the right colleague. That way no important information should ever be lost as a result of the school's

email deletion protocol. If you consider that reasons exist for the protocol not to apply or need assistance in how to retain and appropriately archive data, please contact the Head in advance of the deletion date.

Breach reporting

The law requires the school to notify personal data breaches, if they are likely to cause harm, to the authorities and, in some cases, to those affected. A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This will include almost any loss of, or compromise to, personal data held by the school regardless of whether the personal data falls into a third party's hands. This would include:

- loss of an unencrypted laptop, USB stick or a physical file containing personal data;
- any external hacking of the school's systems, eg through the use of malware;
- application of the wrong privacy settings to online systems;
- misdirected post, fax or email;
- failing to bcc recipients of a mass email; and
- unsecure disposal.

The school must generally report personal data breaches to the ICO without undue delay (ie within 72 hours), and certainly if it presents a risk to individuals. In addition, controllers must notify individuals affected if that risk is high. In any event, the school must keep a record of any personal data breaches, regardless of whether we need to notify the ICO.

If either staff or pupils become aware of a suspected breach, you should notify the Director of Operations (Schools) immediately.

Data breaches will happen to all organisations, but the school must take steps to ensure they are as rare and limited as possible and that, when they do happen, the worst effects are contained and mitigated. This requires the involvement and support of all staff and pupils. The school's primary interest and responsibility is in protecting potential victims and having visibility of how effective its policies and training are. Accordingly, falling victim to a data breach, either by human error or malicious attack, will not always be the result of a serious conduct issue or breach of policy; but failure to report a breach will be a disciplinary offence.

Breaches of this policy

A deliberate breach of this policy will be dealt with as a disciplinary matter using the school's usual procedures. In addition, a deliberate breach may result in the school restricting your access to school IT systems.

If you become aware of a breach of this policy or the e-Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online you should report it to the Director of Operations (Schools). Reports will be treated in confidence.

EATON SQUARE
SENIOR SCHOOL

Acceptance of this policy: Parents/Guardians and Pupils

E-Safety Policy & Acceptable Use Policy for Parents, Pupils Visitors and Staff

Please confirm that you understand and accept this policy by completing below. Parents and pupils can complete the same form).

Please provide name, signature and date below in the appropriate section:

Pupil Name	
Pupil Signature	
Date	

Parent/Guardian 1 Name	
Parent/Guardian 1 Signature	
Date	

Parent/Guardian 2 Name	
Parent/Guardian 2 Signature	
Date	

Please ask your son/daughter to return this form to their Form Tutor.

EATON SQUARE
SENIOR SCHOOL

Acceptance of this policy: Staff/Visitors

E-Safety Policy & Acceptable Use Policy for Parents, Pupils Visitors and Staff

Please confirm that you understand and accept this policy by completing below

Please provide name, signature and date below in the appropriate section:

Staff / Visitor Name	
Staff / Visitor Signature	
Date	

Please return this form to Reception.