INSPIRATIONAL
Box Hill School

E-Safety Policy

Policy Statement

Background
The School recognises that Information Technology, (IT) and the Internet are excellent tools for learning, communication and collaboration. These are accessible within the School for enhancing the curriculum, to challenge pupils, and to support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the School community. It also gives pupils new and exciting opportunities.

However, it is important that the use of IT and the internet is understood and that it is the responsibility of pupils, staff and parents, to use it appropriately and practise good e-safety. It is important that all members of the School community are aware of the dangers of using the internet and how they should conduct themselves online.

The School recognises that it is an important part of the School's role to teach pupils how to stay safe in this online environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of comprising their online reputation.

Box Hill School recognises that internet safety is a child protection and general safeguarding issue.

Scope
E-safety does not just cover the Internet and available resources, but all different types of devices and platforms (e.g. Smartphones devices, wearable technology and other electronic communication technologies). The School understands that some adults and young people will use these technologies to harm children. The School has a duty of care towards staff, pupils or members of the wider School community, to educate them on the risks and responsibilities of e-safety. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This Policy governs all individuals who are given access to the School's IT systems. This could include staff, Governors and pupils however, sections of this policy may not be relevant to certain individuals due to their position, job role or subject to the age of the pupil.

Purpose
This policy aims to be an aid in regulating IT activity in School and provide a good understanding of appropriate IT use that members of the School community can use as a reference for their conduct online outside of School hours. E-safety is a whole-school issue and responsibility.

Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through the School's anti-bullying policy and procedures.

If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures (see the School's Safeguarding Policy).

This Policy is supplementary to the Pupil and Staff ICT Acceptable Usage Policy but should also be read in conjunction with other material listed in appendix 1.

Mandate

Roles and responsibility

The Headmaster, Chief Operating Officer, Deputy Head Pastoral, Designated Safeguarding Lead, Head of IT Services and Governors will ensure that the e-safety policy is implemented and that compliance with the Policy is monitored.

The Governing Body will undertake an annual review of the School's safeguarding procedures and their implementation, which will include consideration of how pupils may be taught about safeguarding, including online safety, through the School's curricular provision, ensuring relevance, breadth and progression.

The Chief Operating Officer will lead on all e-safety matters linked to personal data, infrastructure, software, technical capabilities, filtering and monitoring whilst the Deputy Head Pastoral will lead on all matters linked to safeguarding. The School community recognises that e-safety is everyone's responsibility and that if they have concerns in this area that they will speak to the Chief Operating Officer for technical concerns, the Deputy Head Pastoral, Assistant Head Pastoral or Deputy DSLs for safeguarding concerns.

Please read the pupil and staff ICT Acceptable Usage Policy for further information about the roles and responsibilities for e-safety within the School, including responsibilities for the security of the School's technical infrastructure and filtering systems.

Communicating School policy

This Policy is available on the School website for all to access, when and as they wish. E-safety is integrated into the curriculum in any circumstance where the internet or technology is being used, as well as being specifically addressed in the PSHEE curriculum. On joining the School, newpupils and staff are required to agree to the ICT Acceptable Usage Policy. Existing staff may on occasion be further required to agree this policy when significant changes are made.

Staff receive annual training in online issues as part of the programme of staff safeguarding professional development.

Making use of IT and the internet in School

Using IT and the internet in School brings many benefits to pupils, staff and parents. The Internet is used to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the School's management functions. Technology is advancing rapidly and is now a large part of everyday life, education and business. The School will endeavour to equip pupils with all the necessary IT skills for them to progress confidently between the key stages, into further education, or into a professional working environment once they leave Box Hill School.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils, (some age specific). The School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a School computer or device connected to the School network. The School cannot accept liability for the material accessed, or any consequences of internet access unless found to be negligent.

Expectations of appropriate use of School computers apply to staff and pupils both in and out of lessons. The School will not tolerate any illegal material and will always report illegal activity to the Police, and any sites of concern to the Internet Watch Foundation. If the School discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from their parents and Surrey Police or the Child Exploitation and Online Protection Unit (CEOP). The School will impose a sanction (in line with the Behaviour Policy) on any pupil who misuses technology. In this context misuse may include using technology to bully, harass or to access inappropriate material. The School is also under a duty to report activity suggesting radicalisation under the Prevent Duty.

Parental/Guardian Involvement

Box Hill 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 child when they use electronic equipment at home. The School therefore, arranges discussion evenings for parents when an outside specialist advises about the potential hazards of this increasingly ubiquitous technology and the practical steps that parents can take to minimise the potential dangers without curbing their natural enthusiasm and curiosity of the children. The School also uses its pastoral newsletter *Outside the Box* to share information in this area with parents and guardians.

Teaching pupils how to stay safe

With a dramatic increase in available technologies, the School recognises that education in this area is vital to enable pupils to protect themselves outside of School. We, as a School, need to teach all of the pupils to understand why they need to behave responsibly if they are to protect themselves.

Hence, the pupils are taught how to stay safe online via PSHEE and the wider School curriculum including assemblies. The aim is to help the pupils to adjust their behaviours in order to reduce risks and build resilience, including to radicalisation, with particular regard to the safe use of electronic equipment and the internet. The School's guidance is that pupils (and staff) should always think carefully before they post any information online. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

The School takes seriously its duty to help the pupils understand the risks posed by adults or young people who use the internet and social media to bully, groom, abuse or radicalise other people. Areas such as these are covered within the PSHEE curriculum.

Learning to evaluate internet content

With so much information available online, it is important that pupils learn how to evaluate internet content for accuracy and intent. This is approached by the School as part of digital literacy across all subjects in the curriculum. Pupils will be taught:

- to be critically aware of materials they read, and shown how to validate information before accepting it as accurate, (e.g. “fake news”);

- to acknowledge the source of information used and to respect copyright. The School will take any intentional acts of plagiarism very seriously;
- about the risks associated with using the internet and how to protect themselves and their peers from potential risks;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- the consequences of negative online behaviour; and
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly.

The School provides e-safety guidance to staff to better protect pupils and themselves from online risks and to deal appropriately with e-safety incidents when they occur. Ongoing staff development training includes training on online safety together with specific safeguarding issues including cyberbullying and radicalisation. The frequency, level and focus of such training will depend on individual roles within the organisation, legal changes and requirements.

If staff or pupils discover unsuitable sites then the URL, time, date and content must be reported to the IT Department or any member of staff. Any material found by members of the School community that is believed to be unlawful will be reported to the appropriate agencies via the Head of IT Services or a member of the Senior Leadership Team (SLT). Regular checks will take place to ensure that filtering services and e-safety processes are in place, functional and effective.

The School also provides e-safety guidance to parents on a regular basis.

Managing information systems

The School is responsible for reviewing and managing the security of the IT services and networks that it operates and takes the protection of School data and personal protection of the School community seriously. This means protecting the School network, (as far as is practicably possible), against viruses, hackers and other external security threats. The security of the School information systems and users will be reviewed regularly by the IT Support team and other third parties engaged with the School and led by the Head of IT Services. Anti-Virus and Malware protection software will be updated regularly. Some safeguards that the School takes to secure computer systems are:

- Making sure that unapproved software is not downloaded or installed to any School computers. Files held on the School network will be regularly checked for viruses;
- The use of user logins and passwords to access the School network will be enforced and unique.
- Portable media containing School data or programmes will not be taken off-site without specific permission from the SLT.
- Access to the School systems and documents are controlled, only appropriate access for work purposes will be granted. Requests to access any restricted areas or to access another person’s email accounts will require SLT approval.

For more information on data protection in School, please refer to the School’s Data Protection and Information Security Policy. The School manages personal data in line with statutory requirements. More information on protecting personal data can be found below.

Pupils must not attempt to bypass the School's network or system security by installing or configuring VPN, proxies, web anonymisers or any other solution designed to bypass web filtering and/or provide anonymous access to internet.

The School, just like other organisations, blocks certain sites and routinely monitors all IT activity undertaken on the School's network. The School monitors inappropriate content to provide an alert to potential safeguarding issues. For both staff and pupils, it should be expected that sanctions will be applied for the misuse of School systems and hardware.

Suitable filters are in place to protect from terrorist and extremist material when accessing the internet in School. Regular checks are carried out to ensure the filtering is in place. Any pupil or member of staff who is found to have accessed such sites will be referred to the DSL who will subsequently follow the procedures as laid out in the Prevent duty.

Emails

The School uses email internally for staff and pupils, and externally for contacting parents, and conducting day to day school business and is an essential part of School communication.

Access in School to external personal email accounts may be blocked. The School has the right to monitor emails, attachments and their contents but will only act if there is suspicion of inappropriate use.

School email accounts and appropriate use

Staff should be aware of the following when using email in School:

- Staff should use their School email accounts for School-related matters, contact with other professionals for work purposes and to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.

- Emails sent from School email accounts should be professional and carefully written. Staff are representing the School at all times and should take this into account when entering into any email communications.

- The School permits the incidental use of staff School email accounts to send personal emails if such use is kept to a minimum and takes place substantially out of normal working hours. The content should not include or refer to anything which is in direct competition to the aims and objectives of the School nor should it include or refer to anything which may bring the School into disrepute. Personal emails should be labelled 'personal' in the subject header. Personal use is a privilege and not a right. If the School discovers that any member of staff has breached these requirements, disciplinary action may be taken.

- For any awkward, sensitive, easily misinterpreted situations or anything that may have legal repercussions, staff should have the content of their email checked carefully by their Head of Department or a senior member of staff.

- Staff must tell their Head of Department or a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

- The forwarding of chain messages is not permitted in School.

Pupils should be aware of the following when using email in School:
Pupils will be taught to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class:

- All pupils are provided with a School email account and pupils may only use approved email accounts on the School system during School hours.

- Pupils are warned not to reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission. Excessive social emailing can interfere with learning and in these cases, will be restricted.

Pupils should immediately inform a member of staff if they receive any offensive, threatening or unsuitable emails either from within the School or from an external account. They should not attempt to deal with this themselves.

Published content and the School website
The School website is viewed as a useful tool for communicating School ethos and practice to the wider community. It is also a valuable resource for prospective parents and pupils, current parents, pupils and staff for keeping up to date with School news and events, celebrating whole-school achievements, personal achievements and promoting the School.

The website is in the public domain and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the School community, copyrights and transparency policies.

A team of staff, under the leadership of the Director of Admissions and Marketing are responsible for publishing and maintaining the content of the School website. The website will comply with the School's guidelines for publications including respect for intellectual property rights and copyright. Staff and pupils will be made aware of copyright in respect of material taken from the internet.

Staff and pupils should take care not to publish anything on the Internet that might bring the School into disrepute.

Policy and guidance of safe use of children's photographs and work
Colour photographs and pupils' work bring the School to life, showcase pupils' talents, and add interest to publications both online and in print that represent the School. However, the School acknowledges the importance of having safety precautions in place to prevent the misuse of such material.

Images of pupils and staff will not be displayed in public, either in print or online, without consent, if the use of the image is considered by the School to be privacy intrusive. Whether consent is obtained from the parents or the pupil themselves will depend upon the maturity of the pupil. Please see the School's Taking, Storing and Using Images of Children Policy for more information about the use of photographs and videos

Using photographs of individual children
Most people who take or view photographs or videos of children do so for entirely innocent, understandable and acceptable reasons. Sadly, some people abuse children through taking or using

images, therefore the School has a Taking, Storing and Using Images of Pupils Policy available along with details of current consent forms.
Children may not be approached or photographed while in School or doing School activities without the School's permission, except for parents taking photographs or videos at School events involving their son or daughter for personal use only.

Pupils are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.
Any photographers that are commissioned by the School will be fully briefed on appropriateness in terms of content and behaviour, will wear identification always, and will not have unsupervised access to the pupils.

Complaints of misuse of photographs or video
Parents should follow standard School complaints procedure if they have a concern or complaint regarding the misuse of School photographs. Please refer to the Complaints Procedure for more information on the steps to take when raising a concern or making a complaint. Any issues or sanctions will be dealt with in line with this policy.

Social networking, social media and personal publishing
Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are most vulnerable to being contacted by a dangerous person. It is important that the School educates pupils so that they can make their own informed decisions and take responsibility for their conduct online.

The School has appropriate filtering and monitoring systems in place and hence blocks inappropriate websites. The School aims to block access to potentially harmful and inappropriate material online without an unreasonable level of blocking. The School will normally block/filter access to social networking sites via the School network. The School encourages parents with children under the ages of 13 to follow the guidance of social media sites such as Facebook and not give their child access. Any concerning activity found on such sites by the School will be reported to parents and the website in question will be informed of the account and a request made for its removal.

Social media sites have many benefits, however both staff and pupils should be aware of how they present themselves online. Pupils are taught through PSHEE and the curriculum about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place, (often referred to as a 'digital footprint' or 'digital tattoo'). The School follows general rules on the use of social media and social networking sites in School:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. Pupils are advised never to give out personal details of any kind which may identify them or their location. They are all made fully aware of the School's code of conduct regarding the use of IT technologies and behaviour online.

- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.

- Official School blogs created by staff or pupils/year groups/School clubs as part of the School curriculum will be moderated by a member of staff and must be registered only against a School controlled email account.

- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The School expects all staff and pupils to remember that they are always representing the School and must act appropriately.

- Safe and professional behaviour of staff online will be discussed at staff induction and guidance is provided through the ICT Acceptable Usage Policy.

- Pupils and staff are not permitted to use "live streaming" features, (or equivalent) of social media platforms such as YouTube, Facebook, Snap Chat or Instagram.

Mobile phones and personal mobile electronic devices (Smartphones), including wearable technology

Mobile phones and other personal devices are now an important part of everyone's life and have considerable value, particularly in relation to individual safety. Whilst these devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are that:

- they can make pupils and staff more vulnerable to cyberbullying;

- they can be used to access inappropriate internet material;

- they can be a distraction in the classroom;

- they are valuable items that could be stolen, damaged, or lost;

- they can have integrated cameras, which can lead to child protection, bullying and data protection issues.

Staff/Pupils must follow the School's Mobile Phone Policy for further guidance on this matter. The School actively manages the use of mobile phones; they are banned for Years 7 to 11 during the working day and are collected overnight for younger boarders.

Cyberbullying

Cyberbullying, as with any other form of bullying, is taken very seriously by the School. Cyberbullying can be a pernicious form of bullying because it can be so pervasive and anonymous. It may feel to the victim that there can be no safe haven as they can be targeted at any time or place.

Information about specific strategies to prevent and tackle bullying are set out in the School's Antibullying Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to all members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action. Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and they should not be afraid to come forward.

Proper supervision of pupils plays an important part in creating a safe ICT environment at School but everyone needs to learn how to stay safe outside the School.

Any incidents of cyberbullying will be dealt with in accordance with the Behaviour Policy and, where appropriate, the School's safeguarding and child protection policies and procedures.

Managing emerging technologies

Technology is progressing rapidly, and innovative technologies are emerging all the time. The School will risk-assess any new technologies before they are allowed in School and will consider any educational and pedagogical benefits that they might have. The School keeps up-to-date with modern technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

Visitors

Guest Wi-Fi provision is available for visitors. The IT Support team need to be contacted in sufficiently far in advance to arrange login and password details.

Appendix 1 – Related Documentation

This policy should be read in conjunction with the following policies and publications.

- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Keeping Children Safe in Education
- Behaviour and Behaviour Management Policy
- Complaints Procedure Data Protection Policy
- PSHEE Policy and scheme of work

September 2023
S. Ansell, Chief Operating Officer
Hayley Robinson, Deputy Head Pastoral
Review Date: August 2024