THE Beaulieu Park SCHOOL

E SAFETY POLICY

Committee Responsible	LGB
Lead Staff Member	Principal
Approved by	LGB
Date Approved	Spring 2021
Version	1
Review Date	Spring 2023

CLP CHELMSFORD LEARNING PARTNERSHIP

THE BEAULIEU PARK SCHOOL – E-SAFETY POLICY

E-safety Policy Rationale:

E-safety encompasses Internet technologies and electronic communications such as laptops, tablets, mobile phones and wireless technology. It highlights the need to educate students about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The purpose of Internet use in school is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the school's management information and administration systems. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our school has a duty to provide students with quality Internet access. Students will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

Policy Links

The school's e-safety policy will operate in conjunction with other policies including those for Behaviour, Anti Bullying, Safeguarding Children, Curriculum, ICT, Data Protection and Security.

e-safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- Sound implementation of e-safety policy in both administration and curriculum, including secure school network design and use.
- Safe and secure broadband for learning including the effective management of content filtering.
- National Education Network standards and specifications.

e-safety considers the following technologies: PCs, laptops, tablets, webcams, digital video equipment, mobile phones, portable media players, games consoles and personal digital assistants. All persons either using technology or supervising the use of technology are required to abide by this policy. e-safety requirements relate to school-owned technology and also to personal technologies.

e-safety requirements are applicable during the times whereby the school is opened and the use of any school equipment outside of normal working hours. As well as extended school events, lettings for community use. It is also relevant to residential/off-site events e.g. school trips and visits.

Designated Person for E-Safety Policy

The school will appoint an e-safety coordinator. In many cases this will be the Designated Safeguarding Lead as the roles overlap. The e-safety policy has been agreed by the Leadership Team and approved by the LGB.

Internet: The Benefit to Education

Benefits of using the Internet in education include:

- Fully supports the school's implementation and delivery of a creative International Curriculum to enhance learning opportunities
- Access to world-wide educational resources
- Inclusion in the National Education Network which connects all UK schools
- Educational and cultural exchanges between pupils world-wide
- Access to experts in many fields for pupils and staff
- Professional development for staff through access to national developments, educational materials and effective curriculum practice
- Collaboration across support services and professional associations

- Improved access to technical support including remote management of networks and automatic system updates
- Exchange of curriculum and administration data with the Local Authority and Department for Education DfE.
- Access to learning wherever and whenever convenient.

The school Internet access will be designed expressly for student use and includes filtering appropriate to the age of pupils.

- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use
- Internet access will be planned to enrich and extend learning activities
- Staff should guide students in on-line activities that will support learning outcomes planned for the pupils' age and maturity.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- All new Year 7 parents are provided with an opt out of using the school's computer and internet facilities before their children begin their education at The Beaulieu Park School

Authorised Internet Access

- Our school will comply with copyright law
- The school will maintain a current record of all students who opt out of use of computing and Internet access
- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource
- Parents will be informed that pupils will be provided with supervised Internet access Parents will be asked to sign and return a consent form for pupil access.

Safeguarding Children and Child Protection

This policy is an extension of the safeguarding children and child protection policies. Caution is expressed to the whole school community as regards child safety in the virtual world as well as the real world. Social networking sites, the

uploading of inappropriate web content and cyber-bullying are issues that adults must ensure vigilance and ensure appropriate means are put in place to safeguard and educate our students. It is expected that students are able to develop their own protection strategies for when adult supervision and technological protection are not available.

World Wide Web and Email

If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the network manager and ICT team who are likely to be the most readily available. The Network Manager then can report to the e-safety coordinator, (DSL).

- School will ensure that the use of Internet derived materials by students and staff complies with copyright law.
- Students should be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- The use of the internet is governed by staff signing up on a regular basis to the school IT resource policy, (appendix C). This provides guidelines for all users and the expectations of the school.
- Students may only use approved e-mail accounts on the school system.
- Students must immediately tell a teacher if they receive offensive e-mail.
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- e-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- The school will block/filter access to social networking sites and newsgroups unless a specific use is approved.

- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Students should be advised not to place personal photos on any social network space.
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The School has an extensive and effective filtering system which all staff and students go through. The system also tracks all users on computers in the school and keeps records of searches (Google) they have performed and a complete internet history over the year.

Video Conferencing

IP videoconferencing should use the educational broadband network to ensure quality of service and security rather than the Internet.

- Students should ask permission from the supervising teacher before making or answering a video-conference call.
- Videoconferencing will be appropriately supervised for the students' age.

Managing Emerging Technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed by the network and leadership team. Mobile phones will not be used for personal use during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden and appropriate action taken.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Where possible consent will be obtained from parents/carer's and colleagues to obtain permission to publish pictures of students and staff.

- The Principal or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing Pupils' Images and Work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified or their image misused.
- Students full names will not be used anywhere on the Web site or Blog, particularly in association with photographs.
- Work can only be published with the permission of the students and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- There will be an annual review of security policies, if circumstances require this will be conducted earlier due to the rapidly changing nature of technology. Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998. A regular meeting with the network manager will take place annually to review our e-safety policy.

Assessing Risks

The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access. The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate on a yearly basis.

Handling e-safety Complaints

- Complaints of Internet misuse will be dealt with by a member of the Leadership team.
- Any complaint about staff misuse must be referred to the Principal or DSL.

- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures. Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with Essex Police to establish procedures for handling potentially illegal issues.

Communication of Policy

Students

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

- All staff will be given the School e-safety Policy and its importance explained. They will sign to confirm their understanding and intended compliance
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

Parents' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school Web site.

This policy underlines the school role in ensuring its community is safe and every reasonable steps will be taken to ensure this is the case. However technology may outstrip some of the issue and practicalities discussed here hence the policy will be reviewed on a yearly cycle.

Appendix A Referral process:

Flowchart for Responding to E-Safety Incidents in School

E-Safety Incident

Unsuitable materials
Report to eSCo and/or Principal
If pupil: review incident and decide on appropriate course of action, applying sanctions as necessary
Inappropriate Activity
If staff: review incident and decide on appropriate course of action, applying sanctions as necessary
Debrief
Contact Safeguarding Children Service/ Initial Response Team
Implement changes
Monitor
Review policies and technical tools

Appendix B Student guidelines:

Student guidelines

Think then Click
We ask permission before using the Internet. We only use websites that an adult has chosen. We tell an adult if we see anything we are uncomfortable with. We immediately close any webpage we not sure about. We only e-mail people an adult has approved. We send e-mails that are polite and friendly. We never give out personal information or passwords. We never arrange to meet anyone we don't know. We do not open e-mails sent by anyone we don't know. We do not use Internet chat rooms.

Appendix C e-safety rules:

Staff guidelines

IT Resources Policy

The school has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers.

- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment.
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate.
- Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses.
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network.
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and Privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password.
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet.
- Other computer users should be respected and should not be harassed, harmed, offended or insulted.
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk.
- Computer storage areas and floppy disks will be treated like school lockers. ICT staff may review your files and communications to ensure that you are using the system responsibly.

Internet

- You should access the Internet only for school activities.
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.

- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms should be avoided.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street.
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer.
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

Please read this document carefully. Only once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet will be denied and you will be subject to disciplinary action. Additional action may be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

I have read and understand the above and agree to use the school computer facilities within these guidelines.

Name: _____

Signature: