Victoria Junior School

Policy for e-Safety and Acceptable Computer Use

Approved by GB October 2018
Reviewed and edited February 2019
Approved by GB October 2019
To be approved by GB June 2021
Signed: Chair of GB

Aims

We believe that computers and the internet are an essential to developing children's skills and preparing them for life in the twenty-first century. Computing and internet use is a part of the statutory National Curriculum (2014) and a necessary tool for staff and pupils. The school has a duty to provide pupils with quality Internet access as part of their learning experience.

The e-safety and acceptable use policy aims to ensure that staff and children's use of computers and the internet is appropriate, safe and complies with government and local guidance.

The E-Safety Co-Ordinator

The e-safety co-ordinator will monitor that practice in school with guidance in this document and advise and support staff. They will alert the Headteacher where they believe that the policy has been breached, or where they believe that pupils are being placed in danger by their use of the internet, either deliberately or inadvertently. They will review this policy.

Internet Access within School

The school Internet access is designed for safe pupil and adult use and will include filtering appropriate to the age of pupils. Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use. Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation. Pupils will be shown how to publish and present information to a wider audience. All internet access is supervised by a member of staff. Staff will explain to pupils that they are not allowed to actively attempt or access or distribute unacceptable material on school systems.
The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law. Pupils will be encouraged to cross-check information before accepting its accuracy. Pupils will be taught how to report unpleasant Internet content e.g. using the KIDSMART or CEOP Report Abuse icon. Children will use an appropriate, search engine when accessing the internet.

Smart Phone Use

Pupils are not allowed to access any internet or wi-fi services during the school day by the use of mobile or smart phones. Pupils are allowed to bring mobile phones into school but they must be handed in to the school staff at Breakfast Club or during registration. Phones are placed in a box which is taken to the office and then returned at the end of the day. Pupils are not allowed to access their phones during the school day, any phones not handed in to the office will be confiscated and parents contacted.

Managing Internet Access

No pupil, member of staff or other user is permitted to access material that is illegal or potentially offensive using school systems. All staff and pupils will have an individual log on and passwords which should not be disclosed. Visitors will have a separate log-on.

School ICT systems security will be reviewed regularly. Virus protection will be updated regularly. Security strategies will be discussed with the Local Authority. The technician will complete any updates or security reviews required, under the direction of the e-Safety co-ordinator.

Internet content will be filtered through LGFL. The school will take all reasonable precautions to prevent access to inappropriate 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 computer connected to the school network. The school cannot accept liability for any material accessed, or any consequences of Internet access. The school should audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective. If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-Safety Coordinator. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

All staff will be given the School e-Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user. Staff that manage filtering systems or monitor ICT use will be supervised by senior management and work to clear procedures for reporting issues.

E-mail

Pupils may only use approved e-mail accounts on the school system, via Purple Mash, where they only have access to send e-mails to staff members. Pupils must immediately tell a teacher if they receive an offensive e-mail. Any user of the school e-mail policy must not use the system to communicate offensive, suggestive or defamatory material. In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to

meet anyone without specific permission. Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known. E-mail messages sent and received from school systems should not be considered private. Pupils and staff should expect that emails could be inspected at any time.

Published content and the school website
Staff or pupil personal contact information will not generally be published. The usual contact details given to other agencies should be the school office email address: office@victoria.hounslow.sch.uk . One or two named individuals will take overall editorial responsibility for the website and ensure that content is accurate and appropriate before it is published online.

Publishing pupils' images
Where images of children are published on the school website, the following steps are taken to ensure children's safety:

(i) Parents sign for permission for their child's photograph to be used. Where a parent has not given permission, a child's image will not be used.
(ii) Names will not be used to identify pupils within an image. Care should be taken to ensure that this also includes the filename.
(iii) Where names are used (separately from an image), the name should only be the child's first name. Pupils' full names will not be used anywhere on a school website.

Social networking and personal publishing

Pupils
Pupils will not use any social networking site in school. In units of work on e-safety, in PSHE lessons and in assemblies, they will learn not to give out personal details of any kind which may identify them, their friends or their location. Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

The school will advise parents not to allow children under the age of 13 to use social networking sites, other than those specifically designed for children which have appropriate safeguarding measures.

Staff
Staff should not access social networking sites using school equipment. Where staff use social networking sites outside of school, they should apply the following principles:

(i) Staff should ensure that personal images and information are not publicly accessible, by applying the appropriate security settings.
(ii) Staff should not contact or have pupils, past pupils under the age of 18, or parents/families as 'friends', other than in exceptional circumstances where they have an existing relationship, which predates their knowledge of the family through school. Even in these circumstances, staff should take great care, for example by ensuring that 'friends of friends' (ie other parents/families) cannot access their profile.
(iii) Staff should not post comments relating to the school, other staff, or children/parents on their social networking pages.

Staff should exercise extreme caution when using any social sites as posting anything that compromises either themselves or the school could lead to disciplinary action.

Managing videoconferencing & webcam use
Videoconferencing should use the educational broadband network to ensure quality of service and security.
Videoconferencing and webcam use will be appropriately supervised for the pupil's age.
Remote Learning will be delivered through Zoom is to follow the guidelines outlined in the school's Remote Learning policy. This includes ensuring that meetings are set to private and by invitation only, that participants identities are verified visually by webcam, and that pupils are supervised by an adult at all times.

Managing emerging technologies
Emerging technologies will be examined for educational benefit and, where appropriate, a risk assessment will be carried out before use in school is allowed.

Protecting personal data
Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, sexual orientation, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition.

Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

The school will use secure methods to transfer data to any external third parties, and will require undertakings that any such data is held securely. The school will ensure that any web-based systems it uses, for example for assessment, have appropriate safeguards for data protection in place. Where USB data sticks are used to transfer information, they should be securely encrypted, and virus-scanned each time they are re-introduced to the school network.

Handling e-safety complaints
Complaints of Internet misuse will be dealt with by a senior member of staff. Any complaint about staff misuse must be referred to the headteacher. Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.

Communications Policy
E-Safety rules will be discussed with pupils regularly. Pupils will be informed that network and Internet use will be monitored and appropriately followed up. Learning about e-Safety will form a regular part of ICT provision in all year groups, and is delivered very specifically as part of a unit of work in Year 5.

Wireless Access
Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption. Laptops, netbooks and Ipads which have wireless internet access are set up to allow access to the school network and are managed under LGFL guidelines.