Online Policy

1 Who will write and review the policy?

The school has a designated e-Safety Coordinator (Rose Coburn), who works alongside the designated child protection teachers. They work in collaboration with the Subject Leaders in ICT and PSHCE in order to ensure this policy meets the ever-changing issues relating to the Internet and its safe use.

Our e-safety Policy has been written by the school, building on the school's needs and government guidance. The policy has been agreed by the leadership team and approved by the Governing Body. It will be reviewed regularly. Changes will be made immediately if technological or other developments so require.

2 What is e-Safety?

E-Safety encompasses Internet technologies and electronic communications such as mobile phones. This policy highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experiences.

This policy will operate in conjunction with other school policies including those for ICT, behaviour, bullying, PSHCE and child protection.

This policy has been developed out of guidance issued by the London Borough of Hillingdon Local Safeguarding Board.

TEACHING & LEARNING

3 Why is Internet use important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions.

- Internet use is a part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for students who show a responsible and mature approach to its use.
- The Internet is an essential element in 21st Century life for education, business and social interaction. The school has a duty to provide students with quality ICT teaching and learning experiences, which enable them to be equipped in the world they live in.
- Internet access is a part of pupils' learning experience.
- Pupils use the Internet widely outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

4 How does the Internet benefit education?

Benefits of using the Internet in education include:

- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between pupils world-wide;
- Cultural, vocational, social and leisure use in libraries, clubs and at home;
- 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, professional associations and between colleagues;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to tools of direct communication, including Fronter and video conferencing

5 How can Internet use enhance learning?

- The school Internet access will be designed expressly for pupil 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.
- Internet access will be planned to enrich and extend learning activities. Access levels will be reviewed to reflect the curriculum requirements and age of pupils.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

6 How will pupils learn to evaluate Internet content?

- If staff or pupils discover unsuitable sites the URL (address) and content must be reported to the Internet Service Provider via the ICT co-ordinator. Pupils must follow the procedure for reporting unsuitable Internet content (Appendix I) which is shared with all pupils by their class teacher.
- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- Pupils will be taught to acknowledge the source of information and to respect copyright when using Internet material in their own work.

- The evaluation of on-line materials is a part of every subject.

MANAGING INFORMATION SERVICES

7 How will our ICT system security be maintained?

- The school ICT systems will be reviewed regularly with regard to security.
- Virus protection (Sophos) will be installed and updated regularly.
- Use of data storage facilities by pupils within school is prohibited to protect against virus transfer.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas.
- Files held on the school's network will be regularly checked.
- The ICT manager will ensure that the system has the capacity to take increased traffic caused by Internet use.

8 How will e-mail be managed?

Currently LGfL do not supply individual email addresses for pupils. However, the following applies when they are available for pupils.

- Pupils must tell a teacher immediately if they receive offensive e-mail. The instance will be recorded by the senior leadership team and appropriate sanctions applied.
- Pupils must not reveal personal details of or those of others, or arrange to meet anyone in e-mail or other electronic communication, in line with e-safety guidelines.
- Access in school to external personal e-mail accounts is blocked.
- Excessive social e-mail use can interfere with learning and may be restricted.
- E-mails 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 messages is not permitted.

9 How should Web site content be managed?

- The point of contact on the Web site will be the school address, school e-mail and telephone number. Staff or pupils' personal information will not be published. Staff may publish their email addresses through year group and other newsletters.

- The Headteacher will take overall editorial responsibility and ensure content is accurate and appropriate on all pages directly related to the day-to-day workings of the school. At present editorial responsibility for all other areas of the website is the responsibility of Deborah Selfe

- The Website should comply with the school's guidelines for publications.

- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

10 Can pupils' images or work be published?

- Images which include pupils will be selected carefully and only those children whose written parental permission has been sought will be identifiable.

- Pupils' full names will not be used on the Website when associated with photographs, or in any way which may be to the detriment of pupils.

- Pupil photographs will immediately be removed from the school Website upon request from parents, or other appropriate request.

11 How will social networking and personal publishing be managed?

The school will block access to social networking sites.

Pupils will be advised never to give out personal details of any kind which may identify them and their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.

Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas.

Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. House number, street name or school.

Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Students should be advised not to publish specific and detailed private thoughts.

Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.

Newsgroups will not be made available unless an educational requirement for their use has been demonstrated.

12 How will filtering be managed?

- The school will work in partnership with parents, LGfL, Atomwide, and AzteQ to ensure content is filtered.

- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the ICT Subject Leader. Atomwide will be contacted by Deb Selfe

- The school will ensure filtering methods are in place to keep children safe from all types of inappropriate and unacceptable materials, including terrorist and extremist material.

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

- Any material that the school believes is illegal must be referred to the LGfL, Atomwide, CEOP and Channel

13 How will videoconferencing be managed?
The equipment and network
Video conferencing is not currently used but the following will apply if/when it is.

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

- All videoconferencing equipment in the classroom must be switched off when not
- in use.

- External IP addresses should not be made available to other sites.

- Videoconferencing contact information should not be put on the school Website.

- School videoconferencing equipment should not be taken off school premises without permission. Use over the non-educational network cannot be monitored or controlled.

Users

Videoconferencing should be supervised appropriately for the pupils' age.

Parental permission will be sought for children to take part in videoconferences.

Only key administrators should be given access to the videoconferencing system, web or other remote control page.

Unique log on and password details for the educational videoconferencing services should only be issued to members of staff and kept secure.

Content

- When recording a videoconference lesson, written permission should be given by all sites and participants. The reason for the recording must be given and the recording of videoconference should be clear to all parties at the start of the conference.

- Recorded material shall be stored securely.

- If third-party materials are to be included, check that recording is acceptable to avoid infringing the third party intellectual property rights.

- Videoconferencing is a challenging activity with a wide range of learning benefits.

- Preparation and evaluation are essential to the whole activity.

- Establish dialogue with other conference participants before taking part in a videoconference. If it is a non school site it is important to check that they are delivering material that is appropriate for your class.

14 How can emerging Internet uses be managed?

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

Mobile phones are not to be brought to school by pupils, unless with the agreement of a member of SLT. Mobile phones will be kept in the office in the locked filing cabinet during the day. The sending of abusive or inappropriate text messages is forbidden.

Pupils and parents are made aware of the minimum age for all social networking sites.

Pupils are to inform staff of any inappropriate text messages or social networking content used out of school.

15 How should personal data be protected?

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

- School laptops or USB drives containing personal data will be encrypted.

POLICY DECISIONS

16 How will Internet access be authorised?

All staff and pupils will initially be granted Internet access.

- Parents will be informed that pupils will be provided with supervised Internet
- access.

- Parents will be asked to sign and return a consent form and reasonable use agreement.

- Guidelines relating to Internet safety are visible from all machines with Internet access, throughout the school.

17 How will the risks be assessed?

- In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.

- However, due to the global and linked nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor LGfL can accept liability for the material accessed, or any consequences resulting from Internet use.

- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Methods to identify, assess and minimise risks will be reviewed regularly.

- The Headteacher will ensure that the e-Safety Policy is implemented and compliance with the policy monitored.

18 How will e-safety complaints be handled?

Responsibility for handling incidents will be delegated to a senior member of staff.

- Any complaint about staff misuse must be referred to the Headteacher.

- Pupils and parents will be informed of the complaints procedure.

- Parents and pupils will need to work in partnership with staff to resolve issues.
- As with drugs issues, there may be occasions when the police must be contacted. Early contact could be made to establish the legal position and discuss strategies.

- Sanctions available include:

- interview/counselling by senior member of staff/class teacher/teaching assistants;
- informing parents or carers;
- removal of Internet or computer access for a period, which could prevent access to school work held on the system.

19 How is the Internet used across the community?

The school will liaise with local organisations to establish a common approach to e-safety.
The school will be sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.

COMMUNICATIONS POLICY
20 How will the policy be introduced to pupils?

- Rules for safe internet use will be posted on or near all computer systems with
- Internet access.

- An e-safety training programme will be introduced to raise the awareness and
- importance of safe and responsible Internet use both at school and home.

- Internet safety guidelines will be prominently linked from the home page of the
- school's intranet and Internet sites.

- Pupils will be informed that Internet use will be monitored.

- Instruction in responsible and safe use should precede Internet access.

21 How will the policy be discussed with staff?

- All staff will be given the School e-Safety Policy and its application and importance explained.

- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

- The monitoring of Internet use is a sensitive matter. Staff should only operate
- monitoring procedures on instruction from the Leadership Team.

- Staff training in safe and responsible Internet use, and on the school e-Safety Policy will be provided as required.

22 How will parents' support be enlisted?

- Parents' attention will be drawn to the School e-Safety Policy in newsletters,

- School brochure and on the school website.

- Internet issues will be handled sensitively to inform parents without undue alarm.

- A partnership approach with parents will be encouraged. This will include leaflet distributions, demonstrations, practical sessions and suggestions for safe Internet use at home.

Reviewed: November 2021