ABBEY PRIMARY SCHOOL

E-SAFETY POLICY

The Computing Leads, Ian Sandeman and Helen Lewarne, are E-Safety Co-ordinators. The Computing Leads work in close partnership with the Designated Safeguarding Lead, Stephanie Collings, and WLT ICT Technicians to ensure consistent application of the policy.

Our E-Safety Policy has been written by the school, building on the Local Authority's (LAs) E-Safety Policy and national guidance. It has been approved by governors through the Local Governing Board

1. TEACHING AND LEARNING

1.1 Why Internet Use is Important

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

- Internet use is part of the statutory curriculum and a necessary tool for learning.
- Internet access is an entitlement for pupils who show a responsible and mature approach to its use
- The Internet is an essential element for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their 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.

1.2 How Internet Use Benefits Education

Benefits of using the Internet are:

- 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;
- 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 and professional associations;
- improved access to technical support including remote management of networks and automatic system updates;
- exchange of curriculum and administration data with Sutton and the DCSF;
- access to learning wherever and whenever convenient.

1.3 Enhancing Learning through the Internet

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of the pupils.
- Pupils are 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 will guide pupils in on-line activities that will support the planned learning outcomes for the pupils' age and maturity.
- Pupils will be taught the effective use of the Internet in research, including the skills of knowledge location, retrieval, and evaluation.

1.4 Evaluating the Internet

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.

Despite all filtering, pupils may occasionally access inappropriate material on the Internet. Pupils are taught to close the page and report this immediately to the teacher.

1.5 E-Safety within our 1-1 laptop Scheme.

At Abbey Primary School, we are committed to ensuring the safety and well-being of all our students, this includes the digital world. Where children have been issued with a 1-1 laptop device, they will receive additional e-safety content throughout their digital experience. Please refer to the 1-1 Laptop Scheme Policy for additional details.

2. MANAGING INFORMATION SYSTEMS

2.1 The Maintenance of Security of Information Systems

- Staff act reasonably e.g. the downloading of large files during the working day will affect the service that others receive.
- Staff take responsibility for their network use. For Sutton staff, disregarding the council's Information Security Policy is regarded as a disciplinary matter.
- Workstations are secured against user mistakes and deliberate actions.
- Our server is located in a locked storage cupboard with restricted access.
- The server operating system is secured and kept up to date with critical security patches.

- Virus protection for the whole network, computers and laptops is installed and regularly updated.
- Our wireless network is well managed by the WLT ICT technicians.
- All Internet connections are arranged through London Grid for Learning (LGfL) to ensure compliance with the service Acceptable Use Policy (AUP).
- The LGfL network is configured to prevent unauthorised access between schools.
- Decisions on LGfL security are made by LGfL network administrators.
- Security of the school information systems is reviewed regularly by WLT ICT Technicians.
- Virus protection is reviewed regularly by the WLT ICT Technicians.
- Security strategies are discussed internally with WLT ICT Technicians or others as required.
- Personal data sent over the Internet is encrypted.
- Laptops holding personal data have whole-disk encryption installed.
- Portable media will not be used without specific permission following a virus check.
- Unapproved system utilities and executable files will not be allowed in pupils' work areas or attached to email.
- Files held on the school's network will be regularly checked.
- Storage of copyright music or video files is not permitted.
- The LGFL contact will review system capacity regularly.

2.2 Management of Email

- Pupils may only use approved school email accounts.
- Pupils must immediately tell a member of staff if they receive an offensive email.
- Pupils must not reveal personal details of themselves or others in email communication or arrange to meet anyone without specific permission and then only with a trusted adult present.
- Access to external personal email accounts for pupils is blocked.
- Excessive social email use can interfere with learning and is restricted.
- Email 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, hoaxing or warning is not permitted.

2.3 Management of Published Content

- Our website and blog celebrate pupils' work and promotes the school and its community. Information published is considered from a personal and school security viewpoint.
- Contact details on the website are the school address, office email address and telephone number. Staff or pupils' personal information will not be published.
- Personal email addresses are not published.
- The Headteacher takes overall editorial responsibility and ensures content is accurate and appropriate.
- The DSL monitors comments made on the blog and filters out any that are inappropriate.

2.4 Publishing of Pupils' Images or Work

Only pupils' first names are used and then only when strictly necessary, particularly in association with photographs.

Permission from parents/carers is obtained before images of pupils are electronically published.

2.5 Management of Social Networking and Personal Publishing

Staff are aware that the Internet has emerging online spaces and social networks, which allow pupils and staff to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there is limited control.

Staff should strongly consider the links made to contact by people posting information or linking to their social networking pages. If staff use such services, they should do so by using a nickname, which does not personally identify them. Pupils are encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photograph or address once published.

The school will block all social networking sites.

Newsgroups will be blocked unless a specified use is approved.

Pupils are advised never to give out personal details of any kind, which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, Instant Messenger (IM) or email addresses, full names of friends, specific interests, and clubs etc.

Pupils are advised not to place personal photographs on any social networking space. They are advised to consider how public the information is and consider using private areas. Advice is given regarding background detail in a photograph, which could identify the pupils or his/her location e.g. house number, street name or school (possibly uniform).

Staff must never 'friend' a pupil on his or her personal sites or 'friend' someone who is a 'friend' of a pupil.

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

Pupils are advised not to publish specific and detailed thoughts.

We are aware that bullying can take place through social networking, especially when a space has been set up without a password and others are invited to see the bully's comments.

2.6 Management of Web Filtering

- Levels of Internet access and supervision vary according to the pupil's age and experience.
- Blocking strategies prevent access to a list of unsuitable sites.

- Access monitoring logs the Internet sites visited by individual users (unless blocked by local networking arrangements).
- Key and screen loggers record all text sent by a workstation and analyse it for patterns, often returning false positives requiring manual intervention.
- All web access via the LGFL service is subject to a *minimum* level of filtering.
- We actively work with the WLT ICT Technicians and LGFL administrators to ensure that systems to protect pupils are reviewed and improved.
- If staff or pupils discover unsuitable sites, the Uniform Resource Locator (URL) will be reported to LGFL.
- Senior staff actively work with WLT ICT Technicians to ensure that regular checks are made to ensure that the filtering methods are appropriate, effective, and reasonable.
- If we access any material that we believe is illegal, we will immediately report it to appropriate agencies such as Internet Watch Foundation (IWF) or child Exploitation and Online Protection (CEOP).
- Our filtering strategy is designed by educators to suit the age and curriculum requirements of our pupils, advised by the LA where appropriate.

2.7 Management of Videoconferencing

At present we do not use videoconferencing. The policy will be updated as and when we use this method of communication.

2.8 Management of Emerging Technologies

- Emerging technologies are examined for educational benefits and a risk assessment will be carried out before use in school is allowed.
- Mobile phones are not permitted to be used during lessons or during school time. The sending of abusive or inappropriate text messages is forbidden.
- Staff are issued with the school mobile phone if contact with pupils is needed.

2.9 How is Personal Data Protected?

We have to ensure data held on pupils, families and staff is not manhandled, stolen or misused.

The Data Protection Act 1998 and GDPR 2018 gives individuals the right to know what information is held about them and it provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information. Under the Act every organisation that processes personal information must notify the Information Commissioner's Office unless they are exempt.

The Data Protection Act 1998 and GDPR 2018 applies to anyone who handles or has access to information concerning individuals. Everyone has a legal duty to protect the privacy of information relating to individuals. The Act sets standards, which must be satisfied when processing personal data (information that will identify an individual). The Act also gives rights to the people the information is about i.e. subject access rights lets individuals find out what information is held about them.

The eight principles are that personal data must be:

- processed fairly and lawfully
- processed for specified purposes
- adequate, relevant and not excessive
- accurate and up-to-date
- held no longer than is necessary
- processed in line with individual rights
- kept secure
- transferred only to other countries with suitable security measures.

Personal data will be recorded, processed, transferred and made available according to the GDPR 2018 and further details can be found in our Data Protection Policy.

3. POLICY DECISIONS

3.1 Authorisation of Internet Access

- The school maintains a current record of all staff and pupils who are granted access to the school's electronic communications.
- All staff must read and sign the staff Acceptable Use Policy before using any school ICT resource.
- At Key Stage 1, access to the Internet will be by adult demonstration with occasional directly supervised access to specific, approved on-line materials.
- Key Stage 2 pupils have greater access, under adult supervision.
- Parents are asked to sign and return a consent form for pupil access.

3.2 Risk Assessment

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of the Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor LA can accept liability for the material accessed, or any consequences resulting from Internet use.

- 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.
- The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990.
- Passwords and other security information must never be shared.
- Methods to identify, assess and minimise risks will be reviewed regularly.

3.3 Handling E-Safety Complaints

- A member of the Senior Leadership Team will deal with complaints of Internet misuse.
- Any complaint about staff misuse must be referred to the Headteacher.

- Sanctions for misuse by pupils could include informing parents/carers and the removal of the Internet or computer access or email for a period.

3.4 Internet Use Across the Community

The school is sensitive to Internet related issues experienced by pupils out of school, e.g. social networking sites and offers appropriate advice.

4. COMMUNICATIONS POLICY

4.1 Introducing the Policy to Pupils

- E-Safety will feature on newsletters sent to parents.
- E-Safety rules are posted in rooms with Internet access.
- E-Safety awareness raising meetings are held for pupils.
- Instruction on responsible and safe use precedes Internet access.
- An annual E-Safety project will be held for all pupils.

4.2 Discussing the Policy with Staff

- All staff will be given the school E-Safety Policy and its application and importance explained.
- Staff are aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leaders and have clear procedures for reporting issues.
- Staff training in safe and responsible Internet use and on the school E-Safety Policy will be provided as required.

4.3 Enlisting Parental Support

- Parents' attention will be drawn to the school's E-Safety Policy in newsletters, the prospectus and website.
- Internet issues will be handled sensitively, and parents advised accordingly.
- Partnership with parents will be encouraged. We will hold parents' meetings with demonstrations and suggestions for safe home use.

5. MONITORING OF POLICY

The policy will be reviewed annually by the Abbey Local Governing Board

Approved – **June 2023**
Next review – **June 2024**