LANGFORD VILLAGE COMMUNITY PRIMARY SCHOOL

E-Safety Policy

February 2020

Signed

Peter Greenway CHAIR OF GOVERNORS

Maureen Thompson HEAD TEACHER

PGreenway.

Next review February 2022

Introduction
E-Safety encompasses internet technologies and electronic communications such as mobile phones, tablets, collaboration tools and personal publishing. It 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 experience.
The school's E-safety Policy operates in conjunction with other policies including our: Behaviour Policy, Anti-Bullying Policy and Child Protection and Safeguarding Policy. It also operates in conjunction with the Staff Handbook.

End to End E-Safety
E-Safety depends on effective practice at a number of levels:

- Responsible IT use by all staff and pupils; 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 including the effective management of filtering systems.

Writing and reviewing the E-Safety Policy
The E-Safety Policy relates to other policies including those for the Computing curriculum, Child Protection & Safeguarding, Anti-Bullying and the Behaviour Policy.

- The review of the e-Safety Policy is the responsibility of the Computing/ E- Safety Co-ordinator (Tim Holt) and the Senior Management Team, working in close co-operation with staff. The Head Teacher is one of the school's Designated Safeguarding Officers.
- Our E-Safety Policy is written by the Computing Team and has been agreed by the staff and governors.
- E-Safety issues are included in the Child Protection and Safeguarding Policy and Computing Policy.

Why internet use is important

- 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 internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.

Internet use will enhance learning

- The school internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils are taught what internet use is acceptable and what is not and will be given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.
- Staff should guide pupils in on-line activities that will support the learning outcomes planned for the pupils' age and maturity and educate them in the effective use of the

Internet in research, including the skills of knowledge location, retrieval and evaluation.

Pupils will be taught how to evaluate internet content

- If staff or pupils discover unsuitable sites, the URL (address), time, date and content must be reported in the first instance to one of the school Safeguarding Officers in conjunction with the Computing Co-ordinator.
- Staff should ensure that the use of internet derived materials by staff and by 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.

Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- The school uses broadband with its firewall and filters.

Digital storage

The school uses the main network server for its main secure digital storage.

- Membership is restricted to members of the School community (pupils and staff).
- Usernames and passwords are provided for all members, except younger children who just have usernames.
- Content is regularly monitored by the Computing/ E-Safety Co-ordinator (Tim Holt).

Use of E-mail (where applicable)

- Pupils may only use approved e-mail accounts on the school system. Children are not allowed access to personal e-mail accounts or chat rooms whilst in school.
- Pupils must immediately tell a teacher if they receive an offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- E-mail sent to an external organisation 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.
- Whilst we recognise that some members of staff who live and work within our local community and have friendships with parents, as a result of this, any work-related correspondence should be undertaken through school email addresses and not through personal email or phone numbers.
- 'School Life' is used by the school as the main means of communicating electronically with parents/carers.

Published content and the school web site

- The contact details on the website should be the school address, e-mail and telephone number (and that of the SENCo). Staff or pupils personal information will not be published.
- The School website will be used to provide up-to-date information regarding the School.
- The Senior Leadership Team (SLT) will take overall editorial responsibility and ensure that content is accurate and appropriate. (Phase Leaders are to check that the information being uploaded is factually and grammatically correct).

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Pupils are advised never to give out personal details of any kind that may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.
- Pupils and parents will be advised that the use of social network spaces outside school may be inappropriate for primary aged pupils.
- Contact between staff members, pupils and parents on social networking sites is deemed inappropriate.

Managing filtering

- The school will work in partnership with the service provider to ensure filtering systems are as effective as possible.
- If staff or pupils discover unsuitable sites, the URL, time and date must be reported to the Computing Co-ordinator.
- The Computing Co-ordinator will ensure that checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

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.
- Mobile phones will not be used during lessons or formal school time. The sending of abusive or inappropriate text messages is forbidden.

- Staff have access to a school phone where contact with pupils or parents is required. Staff may not use personal mobile phones to contact parents except on an offsite visit, where this is deemed necessary, and access to a school phone is not possible.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- The Data Protection Act 1998 which states that personal data must be:
- 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
- Only transferred to others with adequate protection.

Authorising internet access

- The school will maintain a current record of all staff and pupils who are granted internet access.
- All staff, including Teaching Assistants must read and sign the School's acceptable user policy before using any school IT resource.
- At FS/Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- A system is in place for pupils to leave mobile phones in the main office if it is essential for them to have access to a mobile phone because they walk home alone.
- Parents will be asked to sign and return a permission form agreeing to comply with the School's parental acceptable user policy.
- Pupils will agree to either the KS1 or KS2 acceptable user policy.

Assessing risks

- 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 international scale and linked nature of 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 Head Teacher and Governors will ensure that the E-Safety Policy is implemented and compliance with the policy monitored.

Handling e-safety complaints

- Complaints of internet misuse will be dealt with by a senior member of staff and the E-Safety Coordinator (Tim Holt) and will be recorded in a log book.
- Any complaint about staff misuse must be referred to the Head Teacher.
- Complaints of a safeguarding nature must be dealt with in accordance with school safeguarding procedures.
- Pupils and parents are informed of the complaints procedure on the school website.
- Non-compliance of pupils acceptable user policy may result in:
  - discussion with class teacher / Head Teacher;
  - informing parents or carers;
  - removal of internet or computer access for a fixed period.

If required, discussions will be held with the Police School Liaison Officer to establish procedures for handling potentially illegal issues.

Community use of the Internet

- The school will be sensitive to internet related issues experienced by pupils out of school, e.g. social networking sites, and offer appropriate advice.
- A bi-annual e-safety presentation to parents is held as part of our on-going e-safety work with children in school.

Introducing and embedding the e-safety policy to pupils

- Rules for internet access will be posted in all networked rooms and on mobile ICT trolleys and regularly reinforced during teaching sessions.
- Pupils will be informed that internet use will be monitored.
- Advice on e-Safety will be introduced at an age-appropriate level to raise the awareness and importance of safe and responsible internet use.

Staff and the e-Safety policy

- The importance of the e-Safety Policy will be highlighted and discussed in staff, team and Governors' meetings. All staff read and sign as having read and understood the policy.
- The importance of the E-Safety Policy will be explained to staff and pupils.
- Staff should be aware that internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Enlisting parents' / carers' support

- Parents'/ carers' attention will be drawn to the School e-Safety Policy in newsletters, via the e-safety page on the school website and via 'School Life' push notifications.

This policy is to be read in conjunction with:

- Child Protection & Safeguarding Policy
- Ant-Bullying Policy
- Behaviour Policy