E-safety Policy

St Levan School E-safety Policy

The school's E-safety co-ordinator is the school's DSL. When the DSL is not on the school site, the DDSL will adopt this role on their behalf.

Our e-Safety Policy has been written by the school. It has been agreed by the school leadership and approved by governors.

The e-Safety Policy and its implementation will be reviewed annually.

1. The Internet in school, rationale and entitlement

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 part of the statutory curriculum and a necessary tool for learning.
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.
pupils need to be able to evaluate Internet information and to take care of their own safety and security.

2. Benefits of using the internet in school

- access to world-wide educational resources including museums and art galleries;
- 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 such as SIMS and seesaw communities
- access to learning wherever and whenever convenient.
- to promote and celebrate the achievements of the school through a website

3. Managing Internet Access

- The school Internet access will be designed expressly for pupil use and will include filtering appropriate to the age of pupils provided by CCC and our provider NCI.
- 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.

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

4. Evaluating content on the Internet

- The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law.
- If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Internet Service Provider via the Computing subject leader and reported to the Headteacher
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

5. Management of email

- Pupils may only use approved e-mail accounts on the school system as part of a class / group.
- Email accounts can only be set-up by the network manager / admin officer with permission from the Headteacher.
- Pupils will not have individual email accounts but use the internal messaging system within the website blogging service.
- Pupils must immediately tell a teacher if they receive offensive message.
- Pupils will not access their own private email accounts unless supervised by a teacher
- 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.

6. Security of the network and online data and filtering

- The security of the school information systems and Internet filtering will be reviewed regularly and is done in partnership with the LA and NCI.
- Virus protection will be updated regularly.
- Personal data sent over the Internet will be encrypted or otherwise secured.
- Unapproved system utilities and executable files will not be allowed in pupils work areas, attached to e-mail.
- Pupils are not allowed to download any files or programs without permission from a member of staff.
- Files held on the school's network will be regularly checked.
- The Computing co-ordinator/network manager will review system capacity regularly.
- Any material that the school believes is illegal must be reported to appropriate agencies CEOP
Child Exploitation and Online Protection Command
- - Government agency

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Staff passwords are created by them and should never be divulged to anyone else
- Staff laptops are a school resource and staff should exercise caution when downloading files. Staff should consult the Headteacher/NCI before downloading/installing programs.

7. Website Content

- The contact details on the website should be the school address, e-mail and telephone number. Staff or pupils personal information must not be published.
- Only the school admin e-mail or the head@ address is given on the site
- The Head teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
-The website should comply with the school's guidelines for publications including respect for intellectual property rights and copyright.
- Images that include pupils will be selected carefully, mainly depicted in group activities
- Pupils full names will not be used anywhere on the website,
- Written permission from parents or carers will be obtained before images of pupils are electronically published.
- The copyright of all material must be held by the school, or be attributed to the owner where permission to reproduce has been obtained.

8. Social Networking

- CCC/NCI will block/filter access to social networking sites as far as possible. Eg Facebook, Bebo and MySpace
- There will be opportunities to use forums/chat rooms in the closed community of school blogging and so guidance will be given to pupils how to develop an online presence and minimise risk to themselves
- Pupils will be taught 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 Messaging (IM) and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils will 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 e.g. house number, street name or school.
- Staff will be advised that they should keep any contact with parents on a professional basis.

- Pupils will be advised on security and encouraged to keep passwords secret, deny access to unknown individuals and instructed how to block unwanted communications.
- Students will be advised not to publish specific and detailed private thoughts.

9. Videoconferencing

- Staff regularly communicate via teams through courses and infrequent parents' evenings.

10.Emerging technologies *e.g. portable devices, mobile phones, game consoles*

- Emerging technologies will be examined for educational benefit and a risk
- An assessment will be carried out before use in school is allowed. Many of these devices have a multitude of different and useful functions and it can be educational to use them in a setting. Teachers will be able to evaluate their use for a particular function
- Mobile phones will not be used during lessons or formal school time to make or receive calls/messages. All pupil mobile phones must be handed into the office on arrival at the site. The sending of abusive or inappropriate text messages is forbidden.
- InfraRed/Bluetooth/ Wireless communication technologies may be useful and will be used after a teacher has decided it has an educational benefit.

11. Assessing the risk

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer.
- CCC/NCI filters content suitable for pupils
- 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 through Personal development lessons stated in our personal development document – July 2023.

12.Procedures when concerns are raised

- Complaints of Internet misuse by pupils will be raised to the Headteacher
- Any complaint about staff misuse must be referred to the head teacher.

- Pupils and parents will be informed of the complaints procedure.
- Pupils will be encouraged to report any e-safety issues to a parent or guardian when at home or a teacher when at school.
- Parents can report any areas of concern directly to a child's class teacher which should then in turn be reported to the DSL/head teacher.
- Parents and pupils will need to work in partnership with staff to resolve issues.

E-safety awareness at St Levan School

Introducing e-safety to pupils

- E-Safety rules will be discussed during all computing lessons.
- Pupils will be informed that network and Internet use will be monitored.
- Instruction in responsible and safe use should precede Internet access.
- An e-safety module will be included in the Computing curriculum and PSHE planning covering both school and home use for every year group
- The rules are as follows

I will:

- **Always keep my personal details to myself**
- **Think carefully when leaving any message online**
- **is it polite?**
- **is it kind?**
- **Does it fall within the school rules?**
- **Report anything that I don't like (to a teacher at school or a parent/guardian at home)**

Introducing e-safety to staff

- All staff will have access to the School e-Safety Policy online and its application and importance explained.
- Staff should be aware that Internet traffic can be monitored and traced to an individual user. Discretion and professional conduct is essential.
- Staff will have clear procedures for reporting issues regarding inappropriate material which should be filtered or removed immediately
- Staff training in safe and responsible Internet use and on the school e-Safety Policy will be provided as required.
- Staff or adults need to ensure they consider the risks and consequences of anything they may post to any web or social networking sites, as inappropriate comments or images can reflect poorly on an individual and can affect future careers.

Introducing e-safety to parents

- Parents' attention will be drawn to the school's e-Safety Policy in newsletters, and on the school website.
- Internet issues will be handled sensitively, and parents will be advised accordingly.
- A partnership approach with parents will be encouraged.
- This will include parent evenings with demonstrations and suggestions for safe home Internet use.

Advice on filtering systems and educational and leisure activities that include responsible use of the Internet will be made available to parents.

Interested parents will be referred to organisations and websites for further information on a leaflet which will also be online on the school website

Helpful links

Childline
http://www.childline.org.uk/
Child Exploitation & Online Protection Centre
http://www.ceop.gov.uk
Internet Watch Foundation
http://www.iwf.org.uk/
Kidsmart
http://www.kidsmart.org.uk/
Think U Know website
http://www.thinkuknow.co.uk/
Family Online Safe Institute
www.fosi.org
Internet Watch Foundation
www.iwf.org.uk

Date policy adopted: January 2022
Reviewed: September 2023