St. Lawrence Primary School

E Safety Policy

Rationale

St Lawrence School appreciates both the benefits and the risks that modern technology can pose to our community and understands that such technology is constantly evolving. The school will deal with E-Safety incidents in line with this policy and associated Behaviour and Anti-Bullying Policies and will inform parents / carers of incidents of inappropriate E-Safety behaviour that take place outside school.

This policy ensures that we have rigorous procedures in place to ensure the safety of our pupils, staff and wider community as well as educating our pupils to become confidence and resilient users of technology.

This policy applies to all members of the St Lawrence School community who have access to and are users of school ICT systems, both in and out of the school.

Roles and Responsibilities

Headteacher

- Will have a duty of care for ensuring the digital safety of members of the school community;
- Is aware of the procedures to be followed in the event of a serious E-Safety allegation being made;
- Will ensure that the E-Safety Co-ordinator and other relevant staff receive appropriate training to enable them to carry out their E-Safety roles and train other staff members as required.

E-Safety Co-ordinator

- Will take day-to-day responsibility for E-Safety issues and has a leading role is establishing and reviewing the school E-Safety policies and documents;
- Will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- Will provide training and advice for staff where required;
- Will liase with ESC as appropriate;
- Will monitor the reports relating to E-Safety incidents and create / maintain a log of incidents outlining any necessary follow-ups.

Computing Co-ordinator and Technical Staff

- Will ensure that the school's technical infrastructure is secure and is not open to misuse or malicious attack;
- Will ensure that the school meets the e-safety technical requirements and any ESC Guidance that may apply;
- Will ensure that any reports of misuse are passed on to the E-Safety Co-Ordinator or Headteacher.

St. Lawrence Primary School

E Safety Policy

Teaching and Support Staff

- Will report any suspected misuse or problem to the Headteacher or E-Safety Co-ordinator for further investigation;
- Will ensure that all professional digital communications between staff and pupils / parents / carers are on a professional level and only carried out using official school systems;
- Will ensure that E-Safety sessions are embedded throughout the curriculum and take place on a regular basis;
- Will ensure that pupils understand and follow the E-Safety and Acceptable Use guidelines;
- Will ensure that pupils are taught research skills and the need to avoid plagiarism as well as to uphold copyright regulations;
- Will monitor the use of digital technology – mobile devices, cameras etc. – in lessons and implement current policies with regard to these devices.

Safeguarding Officer

- Is aware of the potential for serious child protection / safeguarding issues to arise from:

1. sharing of personal data;
2. access to illegal / inappropriate materials;
3. inappropriate online contact with other children / adults / strangers;
4. potential or actual incidents of grooming;
5. cyber-bullying;
6. potential incidents of radicalisation.

Pupils

- Will need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- Are responsible for using the school's digital technology systems in accordance with the Pupil Acceptable Use Policy;
- Should understand the importance of adopting good E-Safety practice both within and outside school and understand that the E-Safety practices taught at school are relevant to their digital actions out of school;
- Should show understanding with regard to using research tools on the internet and have an awareness of the need to avoid plagiarism and uphold copyright regulations.

Parents / Carers

- Are encouraged to support the school in promoting good E-Safety practice both at home and at school, especially regarding digital and video images taken at school events and the use of their children's personal devices at school (where appropriate).

St. Lawrence Primary School

E Safety Policy

Teaching and Learning

Whilst the use of digital technology is a fundamental part of the curriculum, the use of such technology must be balanced by educating pupils to take a responsible approach. The education of pupils with regard to E-Safety is therefore an essential part of the school's E-Safety provision. Children and young people need the help and support of the school to recognise and avoid E-Safety risks and to build their resilience.

E-Safety should be a focus across all areas of the curriculum and staff should reinforce E-Safety messages throughout their teaching. The E-Safety curriculum should be broad, relevant and provide progression.

St Lawrence School is committed to the following:

- The school's Internet access includes filtering appropriate to the age of the pupils;
- Pupils should be encouraged to understand the need and reasoning behind the Pupil Acceptable Use Policy and taught to adopt safe and responsible use both within and outside school;
- Where pupils are allowed to search the internet, staff should be vigilant in monitoring the content of the websites that pupils visit;
- In lessons where use of the internet is planned, it is best practice that pupils are guided towards sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in Internet searches;
- Staff should act as good role models in their use of digital technology;
- To promote a sense of personal responsibility, all pupils will be aware of the Acceptable Use Policy which is displayed in each classroom and in the Computer Suite;
- A record is kept of any cyber-bullying issues or any inappropriate online behaviour; parents are informed of any significant or repeated inappropriate behaviours;
- The school provides advice and information on reporting offensive materials, abuse, bullying etc. and makes this available for pupils, staff and parents as appropriate;
- E-Safety advice for pupils, staff and parents is provided through curriculum activities, letters, newsletters, social media and high-profile events (for example, Internet Safety Evenings);
- Pupils should be taught in lessons to be critically aware of the materials and content that they may access online;
- The school ensures that staff know how to send or receive sensitive and personal data and that they understand the requirement to protect data through password protection or encryption methods;
- The E-Safety Co-Ordinator will receive ongoing training / information to allow him / her to provide updates to the rest of the school community.

Pupils will be taught a range of skills and behaviours appropriate to their age and experience such as:

- Being able to discriminate between fact, fiction and opinion;
- Showing understanding of 'Netiquette' behaviour when using an online environment / email (for example, polite language to be used, keeping personal information private);
- Having an awareness that online 'friends' may not be who they say they are, and to understand why they should be careful in online environments;

- To understand that they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure that they have turned on any privacy settings, where applicable;
- To understand why they may not post pictures or videos of others without their permission;
- To be aware of strategies for dealing with receipt of inappropriate materials;
- To understand why, and how, some people will 'groom' others with inappropriate or illegal motives (older pupils).

Bring Your Own Device*

The educational opportunities offered by mobile technologies are being expanded as a wide range of devices, software and online services become available for teaching and learning, within and beyond the classroom. This has led to the exploration by schools of users bringing their own technologies in order to provide a greater freedom and choice and usability. Use of BYOD should not introduce vulnerabilities into existing secure environments.

- The school will have a set of clear expectations and responsibilities for all users;
- The school adheres to the Data Protection Act principles;
- All users are aware of the Acceptable Use Agreement;
- All network systems are secure and access for users is differentiated;
- Where possible, these devices will be monitored by the school's usual filtering systems whilst being used on the premises;
- All users will have a user-name and password and will keep this safe.

*BYOD is not in place at this time at St Lawrence School but we are considering a trial in the future.

Use of Digital and Video Images

The development of video imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the Internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide opportunities for cyber-bullying to take place. Digital images may remain available on the Internet forever and may cause harm or embarrassment to individuals in the short or longer term. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular, they should recognise the risks attached to publishing their own images on the Internet (for example, on social networking sites);
- In accordance with guidance from ESC, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use. To respect everyone's privacy, and in some cases, protection, these images should not be published or made publicly available on

social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital images;

- Staff and volunteers are allowed to take digital / video images to support educational aims or for the information of parents, but must follow school policies concerning the sharing, distribution and publication of such images. These images should only be taken on school equipment; personal staff devices should not be used for this purpose.
- Pupils must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include images of pupils will be selected carefully and will comply with good practice guidance on the use of such images;
- Pupil's names will not be used anywhere on the website or school social media sites;
- Written permission from parents / carers will be obtained before photographs of pupils are published on the school website and social media sites.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Jersey Data Protection guidelines 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.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for;
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay;
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing";
- It has a data protection policy;
- It is registered as a Data Controller for the purposes of the Jersey Data Protection Regulations;
- Risk assessments are carried out;
- It has clear and understood arrangements for the security, storage and transfer of personal data;
- Data subjects have rights of access and there are clear procedures for this to be obtained;
- There are clear and understood policies and routines for the deletion and disposal of data;
- There is a policy for reporting, logging, managing and recovering from information risk incidents;
- There are clear data protection clauses in all contracts where personal data may be passed to third parties;

- There are clear policies about the use of cloud storage / cloud computing which ensures that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse;
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data;
- Transfer data using encryption and secure password protected devices.

Communications

When using communication technologies, the school is guided by the following in terms of good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email systems are monitored;
- Users must immediately report (to the E-Safety Officer) the receipt of any communication that makes them feel uncomfortable or is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication;
- Any professional digital communication between staff and pupils / parents / carers must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media systems must not be used for work-related communications;
- Pupils in Key Stage 2 will be provided with individual school email addresses for educational use;
- Pupils should be taught about E-Safety issues, such as the risks attached to the sharing of personal details. Pupils should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies;
- Personal information should not be posted on the school website / Facebook page and only official email addresses should be used to identify members of staff.

Social Media

All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools could be held responsible, indirectly, for acts of their employees in the course of their employment. Reasonable steps to prevent predictable harm must be in place.

School staff should ensure that:

- No inappropriate references should be made in social media relating to pupils, parents, carers or members of staff;
- They do not engage in online discussion on personal matters relating to members of the school community;
- Personal opinions should not be attributed to the school or the Education Department;
- Security settings on personal social media profiles are regularly checked to minimise risk and loss of

personal information.

The school's use of social media for professional purposes will be checked regularly by the Headteacher to ensure compliance with the appropriate policies.

Protecting children from the risk of radicalisation should be seen as part of schools' wider safeguarding duties, and is similar in nature to protecting children from other forms of harm and abuse. The Internet and use of social media in particular has become a major factor in the radicalisation of young people. As with other safeguarding risks, staff should be alert to changes in children's behaviour which could indicate that they may be in need of help or protection. As a school, we must ensure that children are safe from terrorist and extremist material when accessing the Internet in schools.

Responding to Incidents of Misuse

It is expected that all members of the school community will be responsible users of digital technology, who understand and follow the school policies. However, there may be times when infringements of the policies take place, through careless or irresponsible or deliberate misuse.

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through the usual behaviour procedures:

- Minor incidents of misuse may be dealt with by the Class Teacher. Any other incidents of misuse, repeated incidents or E-Safety issues will be referred to the E-Safety Officer;
- Any complaint relating to staff misuse must be referred to the Headteacher;
- Complaints of a child protection nature must be dealt with in accordance with the school's Child Protection Policy.

Staff are requested to record the website address of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content (provided that the content does not contain elements of a sexual nature).

CHANGE HISTORY

Version	Date Issued	Issued by	Reason for Change	Presented To (initials to agree policy has been read and understood)	Approved by:	Date
0.1	23.11.17	Kim Banks	Draft			
0.2	05.02.21	Kim Banks	Reviewed – no changes	All staff	Amory Charlesworth	05.02.21
0.3	02.03.23	Kim Banks	Reviewed – no changes	All staff	Amory Charlesworth	02.03.23