St Lawrence Primary School

Internet and E-Safety Policy

Statement of Intent

ICT is an essential resource and plays an important role in the everyday lives of children, young people and adults. Consequently, the use of the Internet as a tool to develop learning and understanding has also become an integral part of school and home life.

Information and Communication Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- E-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies and radio / Smart TVs

Whilst exciting and beneficial both in and out of the context of education, much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies and that some have minimum age requirements (13 years in most cases).

At St Lawrence Primary School, we understand the responsibility to educate our pupils on e-Safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage, and potentially damage the reputation of the school. This can make it more difficult to use technology to benefit learners.

Everybody in the school community has a shared responsibility to secure any sensitive information used in their day to day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

Both this policy and the Acceptable Use Agreement (for all staff, governors, regular visitors [for regulated activities] and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, mobile devices, webcams, whiteboards, digital video equipment, etc.); and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible individuals. Additionally, all security breaches, lost/stolen equipment or data (including remote access Secure ID tokens and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible individuals. The relevant responsible individuals at St Lawrence Primary School are as follows: The Head teacher, The Designated Safeguarding Lead and the Computing Subject Lead.

Anti-virus and anti-spam system

- The school has an up to date anti-virus and anti-spam system provided by Partnership Education and it is monitored and updated weekly.

- If it is suspected that there may be a virus on any school ICT equipment, individuals are to stop using the equipment and contact the Computing Subject Lead immediately.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

Security

- The school gives relevant staff access to its Management Information System, with a unique username and password

- It is the responsibility of everyone to keep passwords secure

- Staff are aware of their responsibility when accessing school data

- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use

- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data

- Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles.

- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used

.Managing e-mail

- The school gives all staff & governors their own e-mail account to use for all school business as a work based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

- Staff & governors should use their school email for all professional communication.

- It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses

- Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes
- Staff must inform the Computing Subject Lead or their line manager if they receive an offensive e-mail
- Pupils are introduced to e-mail as part of the Computing Programme of Study and monitored accordingly.

E-Safety in the Curriculum

ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the pupils on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

- The school has a framework for teaching internet skills in Computing lessons
- The school provides opportunities within a range of curriculum areas to teach about e-Safety
- Educating pupils about the online risks that they may encounter outside school is done informally, when opportunities arise and as part of the e-Safety curriculum
- Pupils are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling and appropriate activities
- Pupils are made aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are also made aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cyber Mentors, ChildLine or CEOPS report abuse button

E-Safety Skills Development for Staff

- Our staff receive information and training on e-Safety and how they can promote the 'Stay Safe' online messages
- New staff receive information on the school's acceptable use policy as part of their induction
- All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community
- All staff are expected to incorporate e-Safety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

Managing the School e-Safety Messages

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used
- The e-Safety policy will be introduced to the pupils at the start of each school year
- The key e-Safety advice will be promoted widely through school displays, newsletters, class activities and so on

  We will participate in Safer Internet Day each year

Internet Use

The internet is an open worldwide communication medium, available to everyone, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school provides pupils with supervised access to Internet resources through the school's internet connectivity

- Staff will preview any recommended sites, online services, software and apps before use

- Searching for images through open search engines is discouraged when working with pupils

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents re-check these sites and supervise this work. Parents will be advised to supervise any further research

- All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources

- All users must observe copyright of materials from electronic resources

- The school utilises a content filter to ensure that all web-based content is suitable for the age range of the children at the school. In addition to this, the Hector the Dolphin safety button is installed on all school devices to ensure that if any content does upset or distress a child they are able to deactivate this content immediately and report it. All children at the school are made familiar with this use of this tool

Parental Involvement

We believe that it is essential for parents/carers to be fully involved with promoting e-Safety both in and outside of school and to be aware of their responsibilities. We consult and discuss e-Safety with parents/ carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website or Facebook page.)

- Parents/carers are expected to sign a Home-School agreement

- The school disseminates information to parents relating to e-Safety where appropriate in the form of;

    - Information evenings
    - Practical training sessions e.g. current e-Safety issues
    - Posters
    - School website information
    - Newsletter items

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any school information accessed from your own PC or removable media equipment is kept secure, and remove any portable media from computers when not attended.

- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access
- Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others
- Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person
- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment
- You must not post on the internet any personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience

Preventing radicalization

The government statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. The school ensures that suitable filtering is in place and more generally, all staff work to equip children and young people with the knowledge to stay safe online, both in school and outside. Internet safety is integral to our ICT curriculum as well as other parts of the curriculum such as PSHE and British Values. As with other online risks of harm, every staff member, governor or other adult associated with the school, is made aware of the risks posed by the online activity of extremist and terrorist groups. This is carried out with regular PREVENT training facilitated by Bedford Borough Council.

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips and, as per the Safeguarding Policy, personal mobile phones are not permitted in the classrooms whilst pupil are present.
- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and other with advance permission from the Headteacher.
- Pupils and staff must have permission from the Headteacher before any image can be uploaded for publication.

Publishing Pupil’s Images and Work

On a child’s entry to the school all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

- On the school website
- in the school prospectus and other printed publications that the school may produce for promotional purposes
- recorded/ transmitted on a video or webcam

in display material that may be used in the school's communal areas

- in display material that may be used in external areas, i.e. exhibition promoting the school

- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

- in publicity for or resulting from inter-school activities held either on site or at another venue

This consent form is considered valid for the entire academic year unless there is a change in the child's circumstances where consent could be an issue.

Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' full names will not be published.

Before posting identifiable student work on the Internet, a check needs to be made to ensure that permission from the parent/carer has been given for work to be displayed.

Storage of Images

- Images/ films of children are stored on the school's secure server
- Images/films of children are to be removed at the end of the academic year in which that child leaves the school, unless such images/ films are or have been used for the purposes of promoting the school.

Signed: ………………………………………………………..
Chair of Governors

Date: 06/02/2019

Review Date: February 2020

Smile and Stay Safe Poster

SMILE and stay safe

Staying safe means keeping your personal details private, such as full name, phone number, home address, photos or school. Never reply to ASL (age, sex, location)

Meeting up with someone you have met online can be dangerous. Only meet up if you have first told your parent or carer and they can be with you

Information online can be untrue, biased or just inaccurate. Someone online my not be telling the truth about who they are - they may not be a ‘friend’

Let a parent, carer, teacher or trusted adult know if you ever feel worried, uncomfortable or frightened about something online or someone you have met or who has contacted you online

Emails, downloads, IM messages, photos and anything from someone you do not know or trust may contain a virus or unpleasant message. So do not open or reply

Primary Pupil Acceptable Use
Agreement / e-Safety Rules

- I will only use ICT in school for school purposes. This includes supervised use of the internet to access games and other leisure content when at Fun4Us club.
- I will only use my class e-mail address or my own school e-mail address for the purpose of e-mailing and not for the registration of an account of any type, without permission from the class teacher
- I will only open e-mail attachments from people I know, or who my teacher has approved
- I will not tell other people my ICT passwords
- I will only open/delete my own files
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible
- I will not look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell a responsible adult immediately
- I will not give out my own/other's details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- I will not sign up to online services until I am old enough to do so
- If I have made a mistake with following any of the above rules I will notify my teacher or a responsible adult immediately.

Dear Parent/ Carer

ICT, including the internet, e-mail and mobile technologies, has become an important part of learning in our school. We expect all children to be safe and responsible when using any ICT.

Please read and discuss these e-Safety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact Mrs Bush or another member of staff.

Please take care to ensure that appropriate systems are in place at home to protect and support your child/ren.

✂---

Parent/ carer signature
We have discussed this document with ……………………………………..........(child's name) and we agree to follow the e-Safety rules and to support the safe use of ICT at school.

Parent/ Carer Signature …….……………………….…………………………….

Class …………………………………. Date ………………………………

Staff, Governor and Visitor
Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents.

- I will only use the school's email and any related technologies for professional purposes or for uses deemed acceptable by the Head or Governing Body
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to pupils
- I will only use the approved, secure e-mail system(s) for any school business
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community to any website or social media site that is not linked to the school
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher
- I will respect copyright and intellectual property rights
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature ………………………………………… Date ……………………

Full Name ……………………………………... (printed)

Job title ………………………………………………………………………