St Leonard's CE Primary School

e-safety policy for pupil use of ICT

September 2022

(to be reviewed in September 2023)

Contents Page

Responsibilities	**3**
E safety Committee	**3**
Internet use and AUPs	**3**
Photographs and videos	**4**
Photographs and videos taken by parents/carers	**4**
Mobile phones and other devices	**4**
Use of e-mails	**5**
Security and passwords	**5**
Data storage	**5**
Reporting	**5**
Infringements and sanctions	**6**
Rewards	**7**
Social networking	**7**
Education	**8**
Monitoring and reporting	**9**
Appendix 1 – AUP's	**10**
Appendix 2 – Parents letter concerning internet use	**18**
Appendix 3 – Audit	**19**
Appendix 4 – Photo permission form	**20**
Appendix 5 – Useful links	**21**
Appendix 6 – Shropshire Council Staff e-safety policy	**22**

Responsibilities

The members of SLT team responsible for e-safety are Mr Luke Bridges

The Governor responsible for e-safety is Mrs Rebecca Rochester

The e-safety co-ordinator is Mr Luke Bridges

The e-Safety co-ordinator is responsible for leading the e-Safety Committee, delivering staff development and training, recording incidents, reporting any developments and incidents and liaising with the local authority and external agencies to promote e-safety within the school community. He/she may also be required to deliver workshops for parents.

Internet use and Acceptable Use Policies (AUP's)

All members of the school community should agree to an Acceptable Use Policy that is appropriate to their age and role. Examples of the AUPS used can be found in appendix 1.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip. This can be found in appendix 2

AUP's will be reviewed annually. All AUP's will be stored centrally in case of breaches of the e-safety policy.

The AUP will form part of the first lesson of ICT for each year group.

Photographs and Video

The use of photographs and videos is popular in teaching and learning and should be encouraged. However, it is important that consent from parents is gained if videos or photos of pupils are going to be used.

If photos/videos are to be used online then names of pupils should not be linked to pupils.

Staff must be fully aware of the consent form responses from parents when considering use of images.

The Consent form used is in appendix 4.

Staff should always use a school camera to capture images and should not use their personal devices.

Photos taken by the school are subject to the Data Protection Act.

NB: Any children for whom parents/carers have not given consent should not be on any photographs at all.

Photos and videos taken by parents/carers.

Parents and carers are not permitted to take photos/videos of **any** children in school events e.g. Sport's days – and as such no photos/videos are shared on any social networking site, such as Facebook, containing images of the children. School take specific – 'safe' - photographs at Christmas and Sports Days to ensure all children are safe and then give these to parents

Covid 19 regulations

As parents are coming onto the car park on KS1/ down the KS 2 drive, to drop off and pick up children, their mobile phones should NOT be out of their pockets/bags.

Mobile phones and other devices

Pupils should not routinely bring mobile phones to school. Only children who are independent walkers are allowed to bring phones to school.

If pupils bring a mobile phone to school, they are expected to switch their phone off when arriving at school and hand it to the class teacher. The class teacher will keep the mobile phones in their desk or other safe place in the classroom. The phones will be returned to the pupils at the end of the day. Pupils should only switch their phone on at the school gate when exiting the school. If pupils are uncertain about how to meet a responsible adult, they should speak to a school leader waiting at the gate or return to school to speak to a member of staff. The behaviour policy will be applied if phones are not used according to this policy.

Pupils are taught how to use social media safely at school. If the school believes that phones are not being used appropriately at school or at home, the school may remove permission for the phone to be brought to school and parents will be contacted. Unkind behaviour, bullying or inappropriate use of a mobile phone outside of school will be dealt with using the school behaviour policy.

Use of e-mails

Pupils should only use e-mail addresses that have been issued by the school and the email system should only be used for school related matters. Pupils are advised to maintain an alternative personal e-mail address for use at home in non-school related matters.

Security and passwords

Passwords should be changed regularly. The system will inform users when the password is to be changed. Passwords must not be shared. Staff must always 'lock' the PC if they are going to leave it unattended (the picture mute or picture freeze option on a projector will allow an image to remain on the screen and also allow a PC to be 'locked').

All users should be aware that the ICT system is filtered and monitored.

Data storage

Only encrypted USB pens are to be used in school for sensitive data and reports. Staff may use unencrypted pens for general use ie power points; teaching frames etc

Reporting

All breaches of the e-safety policy need to be reported to the designated leads for e safety and then recorded by them in the ICT reporting book that is kept in the general office. The details of the user, date and incident should be reported.

Incidents which may lead to child protection issues need to be passed on to the designated teacher immediately – it is their responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues but may require SLT intervention (eg cyberbullying) should be reported to SLT in the same day.

Allegations involving staff should be reported to the Head Teacher. If the allegation is one of abuse then it should be handled according to the DFE document titled 'Dealing with allegations of abuse against teachers and other staff'. If necessary the local authority's LADO (Local Authority Designated Officer) should be informed.

Evidence of incidents must be preserved and retained.

The curriculum will cover how pupils should report incidents (eg CEOP (Child Exploitation and Online Protection Centre) button, trusted adult, Childline)

Infringements and sanctions

Whenever a student infringes the e-Safety Policy, the final decision on the level of sanction will be at the discretion of the school management.

The following are provided as exemplification only:

Level 1 infringements

- Use of non-educational sites during lessons
- Unauthorised use of email
- Unauthorised use of mobile phone (or other new technologies) in lessons e.g. to send texts to friends
- Use of unauthorised instant messaging / social networking sites

[Possible Sanctions: referred to class teacher / e-Safety Coordinator/ confiscation of phone]

Level 2 infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of email after being warned
- Continued unauthorised use of mobile phone (or other new technologies) after being warned
- Continued use of unauthorised instant messaging / social networking sites Use of File sharing software
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not notifying a member of staff of it

[Possible Sanctions: referred to Class teacher/ e-safety Coordinator / removal of Internet access rights for a period / confiscation of phone / contact with parent]

Level 3 infringements

- Deliberately corrupting or destroying someone's data, violating privacy of others
- Sending an email or message that is regarded as harassment or of a bullying nature (one-off)
- Deliberately trying to access offensive or pornographic material

[Possible Sanctions: referred to Class teacher / e-safety Coordinator / Head Teacher / removal of Internet rights for a period / contact with parents]

Other safeguarding actions

If inappropriate web material is accessed:

1. Ensure appropriate technical support filters the site

2. Inform SSCB/LA as appropriate

Level 4 infringements

- Continued sending of emails or messages regarded as harassment or of a bullying nature after being warned
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- Receipt or transmission of material that infringes the conditions of the Data Protection Acts bringing the St Leonards Primary School into disrepute

[Possible Sanctions – Referred to Head Teacher / Contact with parents / possible exclusion / refer to Community Police Officer / LA e-safety officer]

Other safeguarding actions:
1. Secure and preserve any evidence
2. Inform the sender's e-mail service provider if a system other than the school system is used.

Pupils are also informed that sanctions can be applied to e-safety incidents that take place out of school if they are related to school.

Schools are likely to involve external support agencies as part of these investigations e.g. an ICT technical support service to investigate equipment and data evidence, the Local Authority Human Resources team.

Rewards

Whilst recognising the need for sanctions it is important to balance these with rewards for positive reinforcement. The rewards can take a variety of forms – e.g. class commendation for good research skills, certificates for being good cyber citizens etc. Each year group coordinator will indicate these opportunities within the provided planning.

Social networking

Staff and pupils are not permitted to use social networking sites within school. We do however, teach our children about Social Media, it's benefits and its pitfalls. We teach our children in Year 5 and 6 so that they can stay safe.

Education

Pupils

To equip pupils as confident and safe users of ICT the school will undertake to provide:

a). A planned, broad and progressive e-safety education programme that is fully embedded for all children, in all aspects of the curriculum, in all years. b). Regularly auditing, review and revision of the ICT curriculum
c). E-safety resources that are varied and appropriate and use new technologies to deliver e-safety messages in an engaging and relevant manner
d). Opportunities for pupils to be involved in e-safety education e.g. through peer mentoring, e-safety committee, parent presentations etc

Additionally,

a). Pupils are taught in all lessons to be critically aware of the materials / content they access on-line and are guided to validate the accuracy of information
b). There are many opportunities for pupils to develop a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
c). The school actively provides systematic opportunities for pupils / students to develop the skills of safe and discriminating on-line behaviour
d). Pupils are taught to acknowledge copyright and intellectual property rights in all their work.

Staff

a). A planned programme of formal e-safety training is made available to all staff
b). E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
c). An audit of e-safety training needs is carried out regularly and is addressed
d). All staff have an up to date awareness of e-safety matters, the current school e-safety policy and practices and child protection / safeguarding procedures
e). All new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Policy
f). Staff are encouraged to undertake additional e-safety training such as CEOP training or the European Pedagogical ICT Licence (EPICT) E-Safety Certificate
g). The culture of the school ensures that staff support each other in sharing knowledge and good practice about e-safety
h). The school takes every opportunity to research and understand good practice that is taking place in other schools
i). Governors are offered the opportunity to undertake training.

Parents and the wider community

There will be a planned programme of e-safety sessions for parents, carers, etc. This will be planned, monitored and reviewed by the e-safety co-ordinator with input from the e-safety committee.

Monitoring and reporting

a). The impact of the e-safety policy and practice is monitored through the review / audit of e-safety incident logs, behaviour / bullying logs, surveys of staff, students /pupils, parents / carers

b). The records are reviewed / audited and reported to:

- the school's senior leaders
- Governors
- Shropshire Local Authority (where necessary)
- Shropshire Safeguarding Children Board (SSCB) E-Safety Sub Committee (where necessary)

c). The school action plan indicates any planned action based on the above.

Appendices

Appendix 1 – AUP's

AUP for learners in KS1

I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret
- only open pages which my teacher has said are OK
- only work with people I know in real life
- tell my teacher if anything makes me feel scared or uncomfortable on the internet
- make sure all messages I send are polite ○ show my teacher if I get a nasty message
- not reply to any nasty message or anything which makes me feel uncomfortable
- not give my mobile phone number to anyone who is not a friend in real life
- only email people I know or if my teacher agrees
- only use my school email
- talk to my teacher before using anything on the internet ○ not tell people about myself online (I will not tell them my name, anything about my home and family and pets)
- not upload photographs of myself without asking a teacher ○ never agree to meet a stranger

Anything I do on the computer may be seen by someone else.
I am aware of the CEOP report button and know when to use it.

Signed _____

AUP for learners in KS2

When I am using the computer or other technologies, I want to feel safe all the time.

I agree that I will:

- always keep my passwords a secret ○ only use, move and share personal data securely
- only visit sites which are appropriate
- work in collaboration only with people my school has approved and will deny access to others
- respect the school network security ○ make sure all messages I send are respectful
- show a responsible adult any content that makes me feel unsafe or uncomfortable
- not reply to any nasty message or anything which makes me feel uncomfortable
- not use my own mobile device in school unless I am given permission ○ only give my mobile phone number to friends I know in real life and trust
- only email people I know or approved by my school ○ only use email which has been provided by school ○ obtain permission from a teacher before I order online
- discuss and agree my use of a social networking site with a responsible adult before joining
- always follow the terms and conditions when using a site
- always keep my personal details private. (my name, family information, journey to school, my pets and hobbies are all examples of personal details)
- always check with a responsible adult before I share images of myself or others
- only create and share content that is legal
- never meet an online friend without taking a responsible adult that I know with me

I am aware of the CEOP report button and know when to use it.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Signed _____

AUP for any adult working with learners

The policy aims to ensure that any communications technology is used without creating unnecessary risk to users whilst supporting learning.

I agree that I will:

- only use, move and share personal data securely ○ respect the school network security
- implement the schools policy on the use of technology and digital literacy including the skills of knowledge location, retrieval and evaluation, the recognition of bias, unreliability and validity of sources
- respect the copyright and intellectual property rights of others
- only use approved email accounts
- only use pupil images or work when approved by parents and in a way that will not enable individual pupils to be identified on a public facing site. ○ only give permission to pupils to communicate online with trusted users.
- use the ICT facilities sensibly, professionally, lawfully, consistent with my duties and with respect for pupils and colleagues.
- not use or share my personal (home) accounts/data (eg Facebook, email, ebay etc) with pupils
- set strong passwords which I will not share and will change regularly (a strong password is one which uses a combination of letters, numbers and other permitted signs).
- report unsuitable content and/or ICT misuse to the named e-Safety officer ○ promote any supplied E safety guidance appropriately.

I know that anything I share online may be monitored.

I know that once I share anything online it is completely out of my control and may be used by others in a way that I did not intend.

Continued…

I agree that I will not:

- visit internet sites, make, post, download, upload or pass on, material, remarks, proposals or comments that contain or relate to:
  - inappropriate images
  - promoting discrimination of any kind
  - promoting violence or bullying
  - promoting racial or religious hatred
  - promoting illegal acts
  - breach any Local Authority/School policies, e.g. gambling ○ do anything which exposes others to danger
- post any other information which may be offensive to others ○ forward chain letters ○ breach copyright law
- use personal digital recording equipment including cameras, phones or other devices for taking/transferring images of pupils or staff without permission
- store images or other files off site without permission from the head teacher or their delegated representative.

I will ensure that any private social networking sites, blogs, etc that I create or actively contribute to, do not compromise my professional role.

I understand that data protection policy requires me to keep any information I see regarding staff or pupils which is held within the school's management information system private, secure and confidential. The only exceptions are when there is a safeguarding issue or I am required by law to disclose such information to an appropriate authority.

I accept that my use of the school and Local Authority ICT facilities may be monitored and the outcomes of the monitoring may be used.

Signed _____

AUP Guidance notes for schools and governors

The policy aims to ensure that any communications technology (including computers, mobile devices and mobile phones etc.) is used to supporting learning without creating unnecessary risk to users.

The governors will ensure that:

- learners are encouraged to enjoy the safe use of digital technology to enrich their learning
- learners are made aware of risks and processes for safe digital use
- all adults and learners have received the appropriate acceptable use policies and any required training
- the school has appointed an e-Safety Coordinator and a named governor takes responsibility for e-Safety
- an e-Safety Policy has been written by the school, building on the LSCB e Safety Policy and BECTA guidance
- the e-Safety Policy and its implementation will be reviewed annually ○ the school internet access is designed for educational use and will include appropriate filtering and monitoring
- copyright law is not breached
- learners are taught to evaluate digital materials appropriately ○ parents are aware of the acceptable use policy
- parents will be informed that all technology usage may be subject to monitoring, including URL's and text
- the school will take all reasonable precautions to ensure that users access only appropriate material
- the school will audit use of technology establish if the e-safety policy is adequate and appropriately implemented
- methods to identify, assess and minimise risks will be reviewed annually
- complaints of internet misuse will be dealt with by a senior member of staff

Appendix 2 – Parent letter – internet/e-mail use

St Leonard's CE Primary School

Parent / guardian name:……..
Pupil name: …….
Pupil's registration class: ……

As the parent or legal guardian of the above pupil(s), I grant permission for my child to have access to use the Internet, the Virtual Learning Environment, school Email and other ICT facilities at school. I know that my daughter or son has signed a form to confirm that they will keep to the school's rules for responsible ICT use, outlined in the Acceptable Use Policy (AUP). I also understand that my son/daughter may be informed, if the rules have to be changed during the year.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school will take every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. These steps include using a filtered internet service, secure access to email, employing appropriate teaching practice and teaching e-safety skills to pupils.

I understand that the school can check my child's computer files, and the Internet sites they visit. I also know that the school may contact me if there are concerns about my son/daughter's e-safety or e-behaviour. I will support the school by promoting safe use of the Internet and digital technology at home and will inform the school if I have any concerns over my child's e-safety.

I am aware that the school does not permit parents/carers to take photographs and videos of **any** children in school events e.g. Sport's Days and that as such no photos/videos are shared on any social networking site, such as Facebook containing images, of the children. I will support the school's approach to e-Safety and will not take or upload or add any pictures, video or text that could upset, offend or threaten the safety of any member of the school community.

Parent's signature:…… **Date:**…….

Appendix 3 – School audit

Audit

The self-audit should be completed by the member of the Management Team responsible for the e-safety policy.

Is there a school e-safety Policy that complies with Shropshire guidance? Yes

Date of latest update (at least annual): September 2020
The Leadership team members responsible for e-safety are: Luke Bridges

The Governor responsible for e-Safety is: Rebecca Rochester

The designated members of staff for child protection are Luke Bridges
Cat Weaver
Ruth Spencer
Patricia Ashling

The e-Safety Coordinator is: Nicola Carter-Rix

The e-Safety Policy was approved by the Governors in November 2020

The policy is available for staff: Internal server and Website

The policy is available for parents/carers at:

Website: http://www.stleoanrdsprimary.co.uk

Appendix 4 – Photo/video consent

School Name:

Name of child:

Class:

During the year the staff may intend to take photographs of your child for promotional purposes. These images may appear in our printed publications, on video, on our website, or on all three. They may also be used by the local newspapers.

To comply with the Data Protection Act 1998, we need your permission before we take any images of your child. Please answer the questions below then sign and date the form where shown. Please bring the completed form to the ceremony. No photographs of your child will be taken until we are in receipt of this consent.

Please circle your answer

1. May we use your child's image in our printed promotional publications? Yes / No

2. May we use your child's image on the school website/SLG? Yes / No

3. May we record your child's image on our promotional videos? Yes / No

4. May we use your child's image in the local press? Yes / No

Signature: Date:

Your name (in block capitals):

Appendix 5 – Links

(a) Shropshire Council Education Improvement Service documentation

All EIS Service e-safety documentation can be found at:

https://www.shropshirelg.net/esafety/staff/Pages/welcome.aspx

(b) The Safe Use of New Technologies

The Safe Use of New Technologies report is summary of findings from OFSTED based on 35 e-safety inspections carried out in a range of settings.

http://bit.ly/9qBjQO

(**c) 360 degree Safe**

The policy guidance is based upon criteria with the 360 degree safe framework. The framework can be found at:

http://www.360degreesafe.org.uk

Appendix 6

Shropshire Council has developed an e-safety policy for school staff which has been agreed by the following Professional Associations / Trade Unions representing staff in schools:-

- National Union of Teachers
- National Association of Schoolmasters Union of Women Teachers
- Association of Teachers and Lecturers
- National Association of Head Teachers
- Association of School and College Leaders
- UNISON
- GMB

The policy can be found at:

https://www.shropshirelg.net/services/hr/noticeboardnews/Documents/E-Safety%20Policy.pdf