St Lawrence C E Primary School

Acceptable Use Policy
(AUP)
including
Security of Information
E-Safety

September 2022

ICT Acceptable Use Policy (AUP) - Overview

INTRODUCTION

An acceptable use policy (AUP) is a framework for students and their parents, guardians or carers, and the school. As the use of online services and resources grows, so has awareness of the risks and potential dangers which arise from the use of modern communications, technology and the internet.

The objectives of this policy are:

- To promote the safety of learners in our care both in school and elsewhere.
- To ensure all members of the school community are aware of e-safety.
- To encourage safe and responsible use of technology and the internet.

This policy also includes the "Security of Information" and "E-Safety".

EDUCATIONAL BENEFITS OF ICT

At St Lawrence Primary School, we acknowledge that technology continues to change the way we live and work. We aim to utilise the many educational benefits of ICT and use this powerful tool, to provide and expand good quality learning experiences within all aspects of the curriculum, at each key stage. However, we realise the need to understand both positive and negative aspects of its use and ensure pupils have the knowledge and understanding to make informed decisions. To do this requires the co-operation of pupils, as well as staff and governors,

PROTECTING PUPILS- FILTERING

Internet access is filtered by Telford and Wrekin Information Technology Services. This works by means of a 'disallowed' list, so that inappropriate sites are filtered before they get to schools. However, because of the nature of the Internet, there is a possibility that an inappropriate site can be accessed. If this happens, the school should contact Telford & Wrekin ICT Self Services - report a problem (shortcut link found on the start menu, so that the site can be blocked). The incident should also be reported to the headteacher, who may wish to report it to the LA. The child's parents should be informed and, if appropriate, the teacher should have a sensitive chat with the child concerned.

E-MAIL

All KS2 pupils have their own school email accounts. This is provided by Microsoft for free as part of their Office 365 education platform. The Pupils' email accounts are created and maintained by the school and are secure.

THE SCHOOL WEB SITE

Any images of children used on the school website will not be labelled with the children's names. Children will be referred to by first names only, and no personal information about pupils or teachers will be revealed. If parents request that photographs of pupils should not appear on the internet then this will be respected. Our administrators will keep an up-to-date list of these pupils.

CHAT ROOMS AND INSTANT MESSAGING

Pupils will not be allowed to use chat rooms, newsgroups or instant messaging, unless this has a direct bearing on their learning and is closely supervised by a teacher. This should be sanctioned by the headteacher beforehand.

SANCTIONS

Deliberate misuse of computer systems by pupils will be dealt with by the class teacher or the headteacher, and the sanction will be appropriate to the misdemeanour.
Misuse by members of staff will be dealt with as set out in Shropshire LEA's Code of Practice.

E-SAFETY EDUCATION

Before accessing the Internet, children will be continuously taught how to use the Internet sensibly and safely according to the e-safety policy. They will also be introduced to the school's AUPs and be asked to agree to abide by the guidelines given. An internet safety scheme of work can be found in Appendix 7

All members of the school community will be asked to sign a copy of an age appropriate AUP. The AUPs can be found as:

- Appendix 1 - EYFS/KS1 version
- Appendix 2 - KS2 version
- Appendix 3 - Adult version
- Appendix 4 - Governors

PROMOTING AND MAINTAINING AWARENESS

This acceptable use policy will be widely promoted within the school to governors, staff, pupils and parents alike, at an appropriate level.

MONITORING AND REVIEWING THE ACCEPTABLE USE POLICY

Once adopted, this acceptable use policy will be monitored regularly to ensure that it is effective, and reviewed and updated to ensure that it continues to meet the requirements of the school, and any emerging uses of technology.

St Lawrence Primary School
ICT Security of Information and Equipment

Introduction

This ICT security policy is intended for all school staff, including governors, who use or support the school's ICT systems or data. All users of the school ICT systems or data are also covered by this policy.

The objectives of this policy are to:

- Ensure the protection of confidentiality, integrity and availability of school information and assets.
- Ensure all users are aware of and fully comply with all relevant legislation.
- Ensure all staff understand the need for information and ICT security and their own responsibilities in this respect.

Information covers any information, including electronic capture and storage, manual paper records, video and audio recordings and any images, however created.

The School Information Security Officer (SISO) at St Lawrence Primary school is the headteacher, who is responsible for the school's ICT equipment, systems and data, with direct control over these assets and their use, including responsibility for access control and protection. The headteacher will be the official point of contact for ICT security issues.

Additionally the SISO will be responsible for ensuring that:

- Users are made aware of their personal responsibilities for information and ICT security, particularly data of a sensitive nature including photographs.
- The practical aspects of ICT protection are performed such as producing back up copies of data and protecting the physical access to systems and data.

Responsibilities

Users must comply with the school's ICT policy and the requirements of the Data Protection Act 1998, Computer Misuse Act 1990 and copyright, Designs and Patents Act 1988.

All users must be provided with suitable training and documentation, together with adequate information on policies, procedures and facilities to help safeguard systems and data.

It is the responsibility of users to notify the headteacher of any suspected or actual breach of ICT security. In exceptional circumstances, users may report any such breach directly to the Chair of Governors or to Internal Audit.

Although the above roles have been explicitly identified, the handling of secured data is everyone's responsibility.

Adequate procedures must be established in respect of the ICT security implications when changes in personnel occur, e.g. removal of files, log in and retrieval of computer equipment.

Information Asset Owner (IAO)

The information assets held by the school include: personal data for pupils and staff, assessment records, medical information and special educational needs data. An IAO is identified for each asset. The role of the IAO is to understand:

- What information is held and for what purposes
- How information has been amended or added to over time
- Who has access to protected data and why

The IAO is responsible for managing and addressing risks to the information and ensuring that information handling complies with legal requirements and is used to the full to support the delivery of education.

The IAOs are: Mr A. Brannen and Mr J. Brown

Physical Security

- Arrangements should be made through the ICT co-ordinator or headteacher, before the removal of any ICT equipment from its normal location.

- The risks associated with the removal should be made clear and the impact these risks might have made known to the person carrying out the removal e.g. weight of monitors, damage to machines etc.

- All school owned ICT equipment should be recorded.

- An inventory of the school hardware and software is maintained by the ICT technician.

- Computer monitors which display sensitive material, should be positioned in such a way that information stored or being processed cannot be viewed by unauthorised persons.

- Equipment should be sited safely and in such a way as to avoid damage e.g. a lap top is securely placed, (not on pupils' laps) and desktops don't protrude.

- Equipment should be sited to avoid environmental damage from causes such as dust and heat. Servers should be in a temperature controlled, secure environment.

- Sensitive or personal data should not be left in printers or displayed on monitors when away from the desk.

- Sensitive information should only be given to authorised personnel e.g. passwords, user accounts and confidential documents stored in computer files.

- Ensure sensitive data, both paper and electronic, is disposed of properly e.g. destroy disks, shred paper.

- Any sensitive data sent via e-mail should be suitably marked "in confidence."

System Security

Only persons authorised by the SISO are allowed to use the school's ICT systems.

- Users must not make, distribute or use unlicensed software or data.
- Users must not make or send threatening, offensive or harassing messages.
- Users must not create possess or distribute obscene material.
- Users must ensure they have authorisation for private use of the school's computer facilities.
- The ICT co-ordinator and IT technician, together with the headteacher will determine the level of password control.
- Secure passwords should not be revealed to unauthorised persons.
- Passwords should not be obvious or guessable and complexity should reflect the value and sensitivity of the systems and data.
- Passwords should be changed if a suspected breach of security has been noted e.g. an unauthorised person accessing a security password.
- Regular backups of important data should be made e.g. office data, staff data, policies etc.
- To help maintain security of personal and sensitive data, encryption should be used if held on a mobile device that leaves the school premises.

Virus Protection

The IT technician will ensure current and up to date anti-virus (AV) software is applied to all school ICT systems where appropriate.

- Network machines will receive regular updates of AV protection files via the county set up.
- All users take precautions to avoid malicious software that may destroy or corrupt data e.g. checking all incoming email attachments or internet downloads and should be made aware of how to recognise and handle email hoaxes.
- On notification of the need for a critical security patch, these will be applied by the IT technician.
- When reconnecting a home/school laptop to the school network, users should ensure they run the AV update.
- Any suspected or actual virus infection must be reported immediately to the headteacher or IT technician.

Disposal and Repair of Equipment

- The SISO must ensure any personal data or software is obliterated from a PC if the recipient organisation is not authorised to receive the data.

- Disposal of waste information such as print-outs, CDs and memory sticks which hold sensitive data should be shredded or destroyed.

- It is important that any software remaining on a PC being relinquished is legitimate.

- The headteacher must ensure the requirements of the Waste from Electronic and Electrical Equipment (WEEE) Directive are observed.

Security Incidents

All suspected or actual breaches of information or ICT security, including detection of computer viruses, must be reported to the headteacher who should report the incident to the Technology Services Help Desk 01743 252200

St Lawrence Primary School

E-safety and Safety of Users

September 2018

The member of SLT team responsible for e-safety is:	Mr Alan Brannen
The governor responsible for e-safety is:	Ms Zoe Keeling
The e-safety and ICT co-ordinator is:	Mr James Brown

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 college community. He/she may also be required to deliver workshops for parents.

E-Safety Committee

The school safety committee is convened by the e-safety officer. It will meet once per term and will invite a representative of the following groups: SLT, governors, teaching staff, admin staff, IT technician, parents, pupils.

Internet use and Acceptable Use Policies (AUPs)

All members of the school community will sign an Acceptable Use Policy that is appropriate to their age and role.

A copy of the pupil AUP will be sent to parents with a covering letter/reply slip

AUPs will be reviewed annually. All AUPs 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.

The Prevent Duty

The Prevent Duty is the duty in the Counter-Terrorism and security Act 2015 on specified authorities (Schools) in the exercise of their functions, to have due regard to the needs to prevent people from being drawn into terrorism.

The general risks affecting children and young people may vary from area to area, and cording to their age. Schools and childcare providers are in an important position to identify risks within a given local context.

Schools and childcare providers should be aware of the increased risk of online radicalisation, as organisations seek to radicalise young people through the use of social media and the internet.
The 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. Schools should ensure that suitable filtering is in place. More generally, schools have an important

role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE. General advice and resources for schools in internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, all staff needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

The Prevent Duty means that all staff have a duty to be vigilant and where necessary report concerns over use of the internet that includes, for example, the following:

Internet searches for terms related to extremism
Visits to extremist websites
Use of social media to read or post extremist material
Grooming of individuals

All staff should be aware of the following:

1. DfE Prevent Duty
2. DfE briefing note on the use of social media to encourage travel to Syria and Iraq
3. The Channel Panel

The prevent duty requires a schools monitoring and filtering systems to be fit for purpose.

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.

Staff should always use a school camera to capture images and should not use their personal details.
Photos taken by the school are subject to the Data Protection act.

Photos and videos taken by parents/carers.

Parents and carers are permitted to take photos/videos of their own children in school events. They are requested not to share photos/videos from school events on social networking sites if other pupils appear in the background.

The parental letter concerning photographs includes a paragraph concerning posting photos on social networking sites (see appendix 7)

Photos for personal use such as those taken by parents/carers are not subject to the Data Protection Act.

Security and passwords

Pupils and staff should never share passwords and staff must never let pupils use a staff logon. (See Security Policy) 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. Staff need to risk assess any data that they plan to temporarily store on a USB pen to ensure that any potential loss has minimal impact.

Reporting

All breaches of the e-safety policy need to be reported to the head teacher using the school's incident/concern forms.
Incidents which may lead to child protection issues need to be passed on to the designated headteacher immediately – it is his responsibility to decide on appropriate action not the class teachers.

Incidents which are not child protection issues should also be reported to the headteacher the same day.

Allegations involving staff should be reported to the headteacher. 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 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 button, trusted adult, Childline). It is the e-safety coordinators role to ensure the curriculum is taught and that all teachers instruct pupils how to report incidents.

Infringements and sanctions

Whenever a pupil or staff member infringes the E-Safety Policy, the final decision on the level of sanction will be at the discretion of the headteacher.

Other safeguarding actions

If inappropriate web material is accessed:
1. Ensure appropriate technical support filters the site
2. Inform LA as appropriate

Social networking

Pupils

No one should use social networking sites within school hours. Occasionally it may be necessary for members of staff to view contact as a means of checking pupil and parents' activity. This should not be undertaken by members of staff without consent of the headteacher.

Staff

It is recognised that social networking sites have a major role to play in today's society. However, staff must be aware of the following:

- Staff must not place any negative comments about the school on social networking sites.
- Staff must not add pupils as friends in social networking sites
- Staff must not post pictures of school events without the headteacher's consent
- Staff must not use social networking sites within lesson times
- Staff need to use social networking in a way that does not conflict with the GTC code of conduct or Personnel handbook
- Staff should review and adjust their privacy settings to give them the appropriate level of privacy
- Staff should take care adding parents of pupils as friends and ensure that all school matters are kept confidential.

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 meetings is made available to all staff
b) E-safety training is an integral part of Child Protection / Safeguarding training and vice versa
d) An audit of e-safety training needs is carried out regularly and is addressed
e) 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
f) 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 online e-safety training such as CEOP training.

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 is a planned programme of e-safety sessions for parents, carers, etc. This will take the form of a biannual meeting.
The programme 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

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

Appendix 1

Student / Pupil Acceptable Use Policy Agreement Template – for younger pupils (Foundation / KS1)

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

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 _____

Appendix 2

AUP for learners in KS2

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that the *school* will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school* or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- I will only use my own personal devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

I understand that I am responsible for my actions, both in and out of school:

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network /

internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

Student / Pupil Acceptable Use Agreement Form

This form relates to the *student / pupil* Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the school in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Appendix 3

AUP for any adult working with learners

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the *school* will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using *school* ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video

images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the *school*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School /LA Personal Data Policy (or other relevant policy). Where digital

personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix 4

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 5

Parent letter – internet/e-mail use

St Lawrence C of E Primary School

Parent / guardian name:……..

Pupil name: ……

Pupil's 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 permits parents/carers to take photographs and videos of their own children in school events and that the school requests that photos/videos are not shared on any social networking site such as Facebook if the photos/videos contain images of other children. I will support the school's approach to e-Safety and will not 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 6– Links

(a) Shropshire Council Advisory Service documentation

All Advisory 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

www.thinkuknow.co.uk - This website, developed by the Child Exploitation and Online Protection (CEOP) Centre, provides information for young people on how to stay safe on line

www.childnet-int.org - Childnet International's Kidsmart website has a section for young people aged 11 plus, dealing with mobiles, file sharing, chat, trackback (for example, digital footprints) and privacy.

www.ceop.police.uk - The Child Exploitation and Online Protection (CEOP) Centre is dedicated to eradicating the sexual abuse of children.

www.getsafeonline.org – Advice on data security and staying safe on line

Appendix 7 – e-safety Scheme of Work

St.Lawrence Primary School – e-safety Scheme of Work

ANNUAL PROGRAMME	AUTUMN TERM Look at acceptable use policy – children sign and send home Main e safety teaching to be carried out during class assembly and Computing time (if appropriate) in 1st half Autumn Term for ALL phases During Anti Bullying week – 1 session should focus on cyber bullying using Think u know Cyber bullying DVD	SPRING TERM Children to take part in Safer Internet day activities in February	SUMMER TERM E safety questionnaire KS2 only www.wes.networcs.net

	Objectives	Resources
Foundation Stage	○ I know what ICT is. ○ I know when to ask an adult I trust to use ICT equipment. ○ I know that if I see something I am unsure of I can click on Hector.	Based Around Hectors World 5 cartoon videos linked to Hector – Hectors world lesson pack can be downloaded from www.thinkuknow.co.uk
KS1	○ I know that I shouldn't share personal information online ○ I know that not everyone on line may be who they seem ○ I know that we always tell a trusted adult if we have a problem online ○ I know how to be polite online ○ To begin to understand the **SMART** rules. Keep **s**afe-do not give out personal information. Never arrange to **m**eet an on-line friend unless you have a trusted adult. **A**ccepting emails from unknown people can be dangerous.	Based Around Hectors World 5 cartoon videos linked to Hector – Hectors world lesson pack can be downloaded from www.thinkuknow.co.uk Lesson plans and videos based around characters Lee and Kim downloadable from www.thinkuknow.co.uk Introduce the SMART Rules through character Dongle on cbbc www.bbc.co.uk/cbbc/help/web/besmart.shtml

	Reliable-beware people might not be as reliable as they seem. **T**ell a trusted adult if you feel uncomfortable or worried.	
Lower KS2	○ Ways of communicating – focus on use of internet ○ Emailing / communicating safely ○ Guarding your personal information ('Hector' resources) ○ Keeping Safe online ○ Dealing with unkind / unwanted messages. Telling an adult ○ Online stranger danger – dangers of meeting up.	Introduce the SMART Rules through character Dongle on cbbc www.bbc.co.uk/cbbc/help/web/besmart.shtml Look at the know it all resources – 5 video cartoons about Kara and the SMART crew See www.childnet.com/kia/primary/smartadventure/default.aspx
Upper KS2	○ Safe searching / using search engines ○ Bias and discrimination ○ Online Gaming ○ Internet addiction ○ Downloading / uploading – what are the risks? ○ What's on offer? Risks from commerce over the internet	Intro + 5 episodes relating to different areas of e safety www.cybersmart.gov.au/cyberquoll/index.html Think you know – videos and online activities www.thinkuknow.co.uk Also useful video clips where children are asked to make choices on www.bbc.co.uk/cbbc/topics/stay-safe