St Luke's Policy for the Use of digital and video images

Developing safe school web sites

The school website is an important, public-facing communication channel. Many prospective and existing parents find it convenient to look at the school's website for information and it can be an effective way to share the school's good practice and promote its work. Procedures and practice need to ensure website safety.

Use of still and moving images

Care must be taken when using photographs or video footage of pupils on the school website. Consideration should be given to using group photographs rather than photos of individual children. The first name and last name of individuals in a photograph will not be used. This will reduce the risk of inappropriate, unsolicited attention from people outside the school. An easy rule to remember is:

- **If the pupil is named, avoid using their photograph / video footage.**

- **If the photograph /video is used, avoid naming the pupil.**

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film

If showcasing examples of pupils work consider only their first names will be used, rather than their full names.

Only use images of pupils in suitable dress to reduce the risk of inappropriate use.

In many cases, it is unlikely that the Data Protection Act will apply to the taking of images e.g. photographs taken for personal use, such as those taken by parents or grandparents at a school production or sports day. However, photographs taken for official school use, which are likely to be stored electronically alongside other personal data, may be covered by the Data Protection Act. As such, pupils and students should be advised why they are being taken.

A Parental Permission Form should be obtained before publishing any photographs, video footage etc of pupils on the school website, in a DVD or in any other high profile public printed media.

Staff permission should be obtained before photographs/videos are taken for personal use, such as those taken by parents, grandparents or carers at a school production or sports day.

Procedures:

Use of excerpts of pupils' work such as from written work, scanned images of artwork or photographs of items designed and made in technology lessons, allows pupils to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of pupils.

Links to any external websites should be thoroughly checked by staff before inclusion on a school website to ensure that the content is appropriate both to the school and for the

intended audience. Staff should be aware that the content of websites can change substantially, even in a short space of time. All links should be checked regularly, not only to ensure that they are still active, but that the content remains suitable too.

Text written by pupils should always be reviewed before publishing it on the school website. Staff should check that the work doesn't include the full name of the pupil, or reveal other personal information, such as membership of after school clubs or any other details that could potentially identify them. Pupils' work should also be checked to make sure it does not contain any statements that could be deemed defamatory.

Staff should also ensure that the school is not infringing copyright or intellectual property rights through any content published on the website. For example, using images sourced through Google, or using a Trademark for which copyright permission has not been sought.

The school's website should be monitored to ensure they do not contain personal details of staff or pupils.

If the school website is using a webcam – then this must be checked and monitored to ensure misuse does not occur accidentally or otherwise.

If showcasing school-made digital video work, take care to ensure that pupils aren't referred to by full name on the video, and that pupils' full names aren't given in credits at the end of the film.

Digital images – A range of school cameras, laptops and videos are available for Staff use. All photographic images of pupils should be taken and stored on school equipment. If personal specialised equipment is being used for a specific job it should be registered in writing with the school and a clear undertaking that photographs will be transferred to the school network and will not be stored at home or on memory sticks and used for any other purpose than school approved business.

Technical:

Digital images / video of pupils need to be stored securely on the school network and old images deleted after a reasonable period, or when the pupil has left the school.

The school regularly uses video as part of their Visual Literacy work. Staff must be made aware that they do not use software to 'rip-out' sections of copyrighted movies without permission.

There are safe online environments for publishing, such as the LGfL portal or Learning Platform and School 'Book Publishing' websites.

Education:

Staff and pupils must report any inappropriate use of images to the Headteacher or Assistant Headteachers and understand the importance of safe practice. Staff and pupils also need to understand how to consider an external 'audience' when publishing or presenting work.

Policy statements:

In this school:

- The Headteacher takes overall editorial responsibility to ensure that the website content is accurate and quality of presentation is maintained;
- Uploading of information is restricted to the ICT Governor, the School Secretary, the Head teacher and the members of the SLT.
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We gain parental / carer permission for use of digital photographs or video involving their child as part of the school agreement form when their daughter / son joins the school;
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication;
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs;
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking and storing of pictures of pupils;
- Pupils are taught to publish for a wide range of audiences which might include governors, parents or younger children as part of their ICT scheme of work;
- Pupils are taught about how images can be abused in their e Safety education programme;

Social networking and personal publishing

Parents and teachers need to be aware that the Internet has online spaces and social networks which allow individuals to publish unmediated content. Social networking sites can connect people with similar or even quite different interests. Guests can be invited to view personal spaces and leave comments, over which there may be limited control.

For use by responsible adults, social networking sites provide easy to use, free facilities; although often advertising intrudes and may be dubious in content. Pupils should be encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published.

Examples include: blogs, wikis, MySpace, Bebo, Piczo, Windows Live Spaces, MSN space, forums, bulletin boards, multi-player online gaming, chatrooms, instant messenger and many others.

Policy statements:

- The schools will block/filter access to social networking sites.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc.
- Pupils should be advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location eg. house number, street name or school.
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis.
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.
- Students should be advised not to publish specific and detailed private thoughts.
- Schools should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments.

Acceptable Use Policy (AUP): Staff Agreement Form

This policy covers the use of digital technologies in school: email, Internet, intranet and network resources, software, handheld devices, equipment and systems.

- I will only use the school's digital technology resources and systems for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will not reveal my password(s) to anyone.
- I will log out of or lock the screen when leaving an office or classroom to protect data.
- I will not allow unauthorised individuals to access email / Internet / intranet / network, or other school / LA systems.
- I will ensure all documents, data etc., are saved, accessed and deleted in accordance with the school's network and data security and confidentiality policy.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will only use the approved, secure email system for any school business. (Which is currently: LGfL StaffMail)
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Headteacher.
- I will not download any software or resources from the Internet that can compromise the network, or are not adequately licensed.
- I will not connect a computer, laptop or other device, to the network / Internet that does not have up-to-date anti-virus software.
- I will keep any 'loaned' equipment up-to-date, using the school's recommended anti-virus, firewall and other ICT 'defence' systems.
- I will not use personal digital cameras or any device with camera capabilities for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will not store images of pupils on personal equipment. All images of pupils will be stored only on school equipment.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with or associated with my professional role or the school.
- I agree and accept that any computer, laptop, handheld device loaned to me by the school is provided solely to support my professional responsibilities.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption, such as by using an encrypted USB flash drive, and that I follow school data security protocols when using any such data at any location.

- I understand that data protection policy requires that any information seen by me with regard to staff or pupil information, held within the school's information management system, will be kept private and confidential, EXCEPT when it is deemed necessary that I am required by law to disclose such information to an appropriate authority.
- I will embed the school's online safety curriculum into my teaching.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded.
- I understand that all Internet usage / and network usage can be logged and this information could be made available to my manager on request.
- I understand that failure to comply with this agreement could lead to disciplinary action.

User Signature

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school's most recent Acceptable Use Policy and Online Safety Policy.

I agree to abide by the school's most recent Acceptable Use Policy.

I wish to have an email account; be connected to the Intranet & Internet; be able to use the school's ICT resources and systems.

Signature …… Date ……

Full Name …….... (printed)

Job title ……

St Luke's C of E Primary Policy for Managing ICT Equipment

Using the school network, equipment and data safely: general guidance

The computer system / network is owned by the school and is made available to students to further their education and to staff to enhance their professional activities including teaching, research, administration and management.

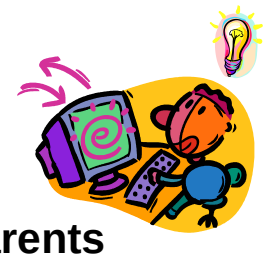
The school reserves the right to examine or delete any files that may be held on its computer system or to monitor any Internet or email activity on the network.

Policy / Procedure statements:

To ensure the network is used safely this school:

- Ensures staff read and sign that they have understood the school's e-safety Policy. Following this, they are set-up with Internet and email access and are given an individual network log-in username and password;
- Provides pupils with an individual network log-in username. From Year 2 they are also expected to use a personal password;
- Makes it clear that staff must keep their log-on username and password private and must not leave them where others can find;
- Makes clear that no one should log on as another user – if two people log on at the same time this may corrupt personal files and profiles;
- Has set-up the network with a shared work area for pupils and one for staff. Staff and pupils are shown how to save work and access work from these areas;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that the computers are switched off at the end of the day.
- Has blocked access to unsuitable Websites.
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;
- Makes clear that staff are responsible for ensuring that all equipment that goes home has the anti-virus and spyware software maintained up-to-date and the school provides them with a solution to do so;
- Makes clear that staff are responsible for ensuring that any laptop loaned to them by the school, is used solely to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by ICT technician, equipment installed and checked by approved Suppliers or LA electrical engineers (Bits) or ICT technician.
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role.

- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school / LA approved systems: e.g. teachers access their area / a staff shared area for planning documentation via Platform Learning
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support or SIMS Support through LA systems; Education Welfare Officers accessing attendance data on specific children.
- Provides pupils and staff with access to content and resources through the approved Learning Platform which staff and pupils access using their Shibboleth compliant username and password.
- Uses the DfES secure s2s website for all CTF files sent to other schools;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA;
- Follows LA advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- Reviews the school ICT systems regularly with regard to security.



St Luke's E-Safety Agreement Form for Parents

Parent / guardian name: _____

Pupil name(s): _____

As the parent or legal guardian of the above pupil(s), I grant permission for my daughter or son to have access to use the Internet, LGfL email and other ICT facilities at school.

I know that my daughter or son has signed an e-safety agreement form and that they have a copy of the 12 'rules for responsible ICT use'.

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 an educationally filtered service, restricted access 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, and that if they have concerns about their e-safety or e-behaviour that they will contact me.

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

Parent / guardian signature: _____

Date: ___/___/___

Use of digital images - photography and video: I also agree to the school using photographs of my child or including them in video material, as described in the document 'Use of digital and video images'. I have read and understood this document. I understand that images will only be used to support learning activities or in publicity that reasonably promotes the work of the school, and for no other purpose. I also understand that while on school premises I am only able to take photographs/videos of my child when permission has been granted by the Headteacher.

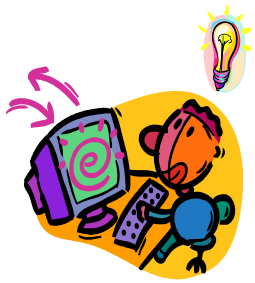
Parent / guardian signature: _____ **Date: ___/___/___**

Keeping safe: stop, think, before you click!

12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only delete my own files.
- I will not look at other people's files without their permission.
- I will keep my login and password secret.
- I will not bring files into school without permission.
- I will ask permission from a member of staff before using the Internet and will not visit Internet sites I know to be banned by the school.
- I will only e-mail people I know, or my teacher has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I have permission or I know and trust the person who has sent it.
- I will not give my home address, phone number, send a photograph or video, or give any other personal information that could be used to identify me, my family or my friends, unless my teacher has given permission.
- I will never arrange to meet someone I have only ever previously met on the Internet or by email or in a chat room, unless my parent, guardian or teacher has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will tell a teacher / responsible adult.



St Luke's Pupil Agreement

Keeping safe: stop, think, before you click!

Pupil name: _____

I have read the school 'rules for responsible ICT use'. My teacher has explained them to me. ☐

I understand these rules are there to help keep me safe, and my friends and family safe. I agree to follow the rules. ☐

This means I will use the computers, Internet, e-mail, online communities, digital cameras, video recorders, and other ICT in a safe and responsible way. ☐

I understand that the school can check my computer files, and the Internet sites I visit and that if they have concerns about my safety, that they may contact my parent / carer. ☐

Pupil's signature _____

Date: ___/___/___

Think before you click

S 

I will only use the Internet and email with an adult

A 

I will only click on icons and links when I know they are safe

F 

I will only send friendly and polite messages

E 

If I see something I don't like on a screen, I will always tell an adult

My Name:

My Signature:

SL LUKE'S C of E PRIMARY SCHOOL

POLICY OF ICT INFRINGEMENT

How will infringements be handled?

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

Students

Category A 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

Sanctions: ***refer to class teacher and/or Headteacher***

Category B 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 / chatrooms, social networking sites, NewsGroups
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Sanctions: ***refer to class teacher and Headteacher -*** *removal of Internet access rights for a period /contact with parent*

Category C infringements

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

Sanctions: ***refer to class teacher and Headteacher -*** *removal of Internet and/or Learning Platform access rights for a period / contact with parents*

Category D infringements

- Continued sending of emails or MSN 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
- Bringing the school name into disrepute

*Sanctions – **Refer to Head Teacher / Contact with parents** / possible exclusion / removal of equipment / 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

Staff

Category A infringements (Misconduct)

- Excessive use of Internet for personal activities not related to professional development e.g. online shopping, personal email, instant messaging etc.
- Use of personal data storage media (e.g. USB memory sticks) without considering access and appropriateness of any files stored.
- Not implementing appropriate safeguarding procedures.
- Any behaviour on the world wide web that compromises the staff members professional standing in the school and community.
- Misuse of first level data security, e.g. wrongful use of passwords.
- Breaching copyright or license e.g. installing unlicensed software on network.

*[Sanction - **referred to line manager / Headteacher**. Warning given.]*

Category B infringements (Gross Misconduct)

- Serious misuse of, or deliberate damage to, any school / Council computer hardware or software;
- Any deliberate attempt to breach data protection or computer security rules;
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent;
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1988;
- Bringing the school name into disrepute.

*[Sanction – **Refer to Headteacher / Governors and follow school disciplinary procedures;** report to LA Personnel/ Human resources, report to Police]*

Other safeguarding actions:

- Remove the PC to a secure place to ensure that there is no further access to the PC or laptop.

- Instigate an audit of all ICT equipment by an outside agency, such as the schools ICT managed service providers - to ensure there is no risk of pupils accessing inappropriate materials in the school.
- Identify the precise details of the material.

If a member of staff commits an exceptionally serious act of gross misconduct they should be instantly suspended. Normally though, there will be an investigation before disciplinary action is taken for any alleged offence. As part of that the member of staff will be asked to explain their actions and these will be considered before any disciplinary action is taken.

The schools may 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.

Child Pornography found?

In the case of Child Pornography being found, the designated safeguarding lead should be notified and the procedures for dealing with allegations of abuse against staff followed. The member of staff should be **immediately suspended** and the Police should be called: see the free phone number **0808 100 00 40** at: http://www.met.police.uk/childpornography/index.htm

Anyone may report any inappropriate or potentially illegal activity or abuse with or towards a child online to the Child Exploitation and Online Protection (CEOP):

http://www.ceop.gov.uk/reporting_abuse.html

http://www.iwf.org.uk

How will staff and students be informed of these procedures?

- They will be fully explained and included within the school's e-safety / Acceptable Use Policy. All staff will be required to sign the school's e-safety Policy acceptance form;
- Pupils will be taught about responsible and acceptable use and given strategies to deal with incidents so they can develop 'safe behaviours'. Pupils will sign an age appropriate e-safety / acceptable use form;
- The school's e-safety policy will be made available and explained to parents, and parents will sign an acceptance form when their child starts at the school.
- Information on reporting abuse / bullying etc will be made available by the school for pupils, staff and parents.
- Staff are issued with the 'What to do if?' guide on e-safety issues.