St. Luke's CEVA Primary School Digital Policy Incorporating Online Safety & GDPR

We are a Christian school that serves a diverse community and works in partnership with parents to develop the whole child.

November 2021

A**ims -** Online Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences. The school's online safety policy will operate in conjunction with other policies including those for Behaviour, Bullying, Curriculum, Data Protection and Safeguarding. Online Safety depends on responsible ICT use by all staff and pupils. It also requires sound implementation of Online safety policy in both administration and curriculum, including secure school network design and use accompanied by **s**afe and secure broadband from the London Grid for Learning including the effective management of content filtering.

Contents

Online Safety Audit –Primary Schools

This quick self-audit will help the senior leadership team (SLT) assess whether the online safety basics are in place.

Has the school an Online -Safety Policy that complies with CYPD guidance?	**Yes**
Date of latest update: **Nov. 2021**	
The Policy was agreed by governors on:	
The Policy is available for staff **on website and in main office and**	
And for parents: **School Website & in paper form from the office**	
The Designated Safeguarding Lead (DSL) is: **Matt Hipperson HT**	
The Online Safety Coordinator is: **Matt Hipperson HT**	
Has Online safety training been provided for both pupils and staff?	**Sept. 2021**
Is the Think U Know training being considered?	**Yes**
Do all staff sign an ICT Code of Conduct on appointment?	**Yes**
Do parents sign and return an agreement that their child will comply with the School Online Safety Rules?	**Yes**
Have school Online Safety Rules been set for pupils?	**Yes**
Are these Rules displayed in all rooms with computers?	**Yes**
Internet access is provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access.	**Yes**
Has the school filtering policy has been approved by SLT?	**Yes**
Is personal data collected, stored and used according to the principles of the GDPR UK Act?	**Yes**

School Online safety Policy

The school has appointed an Online safety coordinator, the Designated Child Protection Officer Matt Hipperson. Our Online safety Policy has been written by the school, building on the Sheffield Children and Young Peoples' Government Directorate guidance. It has been agreed by the senior leadership team and approved by governors.

The Online safety Policy will be reviewed annually. This policy will next be reviewed Jan 2023.

Why is Internet Use Important?

The purpose of Internet use in school is to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management information and administration roles.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business and social interaction. Access to the Internet is therefore an entitlement for pupils who show a responsible and mature approach to its use. Our school has a duty to provide pupils with quality Internet access. Pupils will use the Internet outside school and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet Use Benefit Education?

Benefits of using the Internet in education include:

- access to world-wide educational resources including museums and art galleries;
- inclusion in the National Education Network which connects all UK schools;
- educational and cultural exchanges between pupils world-wide;
- access to experts in many fields for pupils and staff;
- professional development for staff through access to national developments, educational materials and effective curriculum practice;
- collaboration across support services and professional associations;
- improved access to technical support including remote management of
- networks and automatic system updates;
- exchange of curriculum and administration data with the Local Authority and DFE access to learning wherever and whenever convenient.

How can Internet Use Enhance Learning?

- The school Internet access will be designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Internet access will be planned to enrich and extend learning activities.

- Staff will guide pupils in on-line activities that will support learning outcomes planned for the pupils' age.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will regularly learn about online safety across the computing curriculum, they will participate in externally led workshops on how to make best and safest use of modern technology.

Authorised Internet Access

- The school will maintain a current record of all staff and pupils who are granted Internet access. All staff must read and sign the 'Acceptable ICT Use' document to cover using any school ICT resource.
- Parents will be informed that pupils will be provided with supervised internet access.
- Parents will be asked to sign and return a consent form for pupil access.

World Wide Web

- If staff or pupils discover unsuitable sites, the URL (address), time, content must be reported to the LGFL helpdesk via the DSL.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright law.
- Pupils will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy.

Email

- Staff may only use approved e-mail accounts on the school system.
- Staff must immediately tell a teacher if they receive offensive e-mail.
- Staff must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Whole class or group e-mail addresses should be used in school
- Access in school to external personal e-mail accounts may be blocked.
- E-mail sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper.
- The forwarding of chain letters is not permitted.

Social Networking

- School does block/filter access to social networking sites through LGFL and newsgroups unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location
- Pupils will be advised not to place personal photos linked to

their name on any social network space.

- Pupils will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Pupils should be encouraged to invite known friends only and deny access to others.

Filtering

The school will work in partnership with the Local Authority, LGFL and the internet provider to ensure filtering systems are as effective as possible.

Video Conferencing

- Video conferencing through Google Meets, Zoom or Teams should use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should only use video conferencing under the supervision of the class teacher.

Mobile Technology

- **Staff should not use personal mobile phones/digital cameras to take pictures or videos of children, this can be done only on school owned iPads or cameras. Staff use of mobile phones on the premises is governed by statement in the staff handbook. Mobile phones are not permitted for use anywhere in school, around or in the view of the children – except by person in charge. This applies to all members of staff and other visitors to the school except the HT and anyone deputising in his absence. Mobile phones may only be used in office areas, staffroom etc. The only exception to this is staff taking a mobile phone with them on a school trip/visit outside of school, for use in emergencies & only if school phone isn't working.**
- **Children who bring mobile phones to school are required to hand them in to their classroom staff every morning and devices are collected at home time.**

The Prevent Duty and Online safety

All schools have a duty to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. We have an important role to play in equipping children to stay safe on line. Internet safety is integral to our computing curriculum. Our staff are aware of the risks posed by online activity of extremists and have a duty to take action if they believe the well being of any pupil is being compromised.

Published Content and the School Web Site

- The contact details on the Web site should be the school address, e-mail and telephone number. Staff or pupils personal information will not be published.
- The headteacher or nominee will take overall editorial responsibility and ensure that content is accurate and appropriate.

- Any photos taken by school staff should be stored in a shared area and not in a personal account.

Publishing Pupils' Images and Work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be clearly identified.
- Pupils' full names will not be used anywhere particularly in association with photographs.

- Written permission from parents or carers will be obtained before photographs of pupils are published on the school Web site. This is to be done on admission and periodically updated.
- Work can only be published with the permission of the pupil and parents.

Information System Security

- School ICT systems capacity and security will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Security strategies will be discussed with the Local Authority.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the UK GDPR incorporating the Data Protection Act 2018.

Assessing Risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor London Borough of Newham can accept liability for the material accessed, or any consequences of Internet access.
- LGFL filter internet access and keep records of what is accessed as well as managing broadband in liason with Virgin Media. The majority of inappropriate sites have a blanket ban with some sites e.g. You Tube only accessible from staff log-ins.
- It is responsibility of the teacher to view any You Tube sites before the lesson so no inappropriate results may come up.
- The school should audit ICT use to establish if the Online safety policy is adequate and that the implementation of the Online safety policy is appropriate.

Handling Online safety Complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the Headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.
- Discussions will be held with the Police Youth Crime Reduction Officer to establish procedures for handling potentially illegal issues.

Communication of Policy

Pupils

- Rules for Internet access will be posted in all networked rooms.
- Pupils will be informed that Internet use will be monitored.

Staff

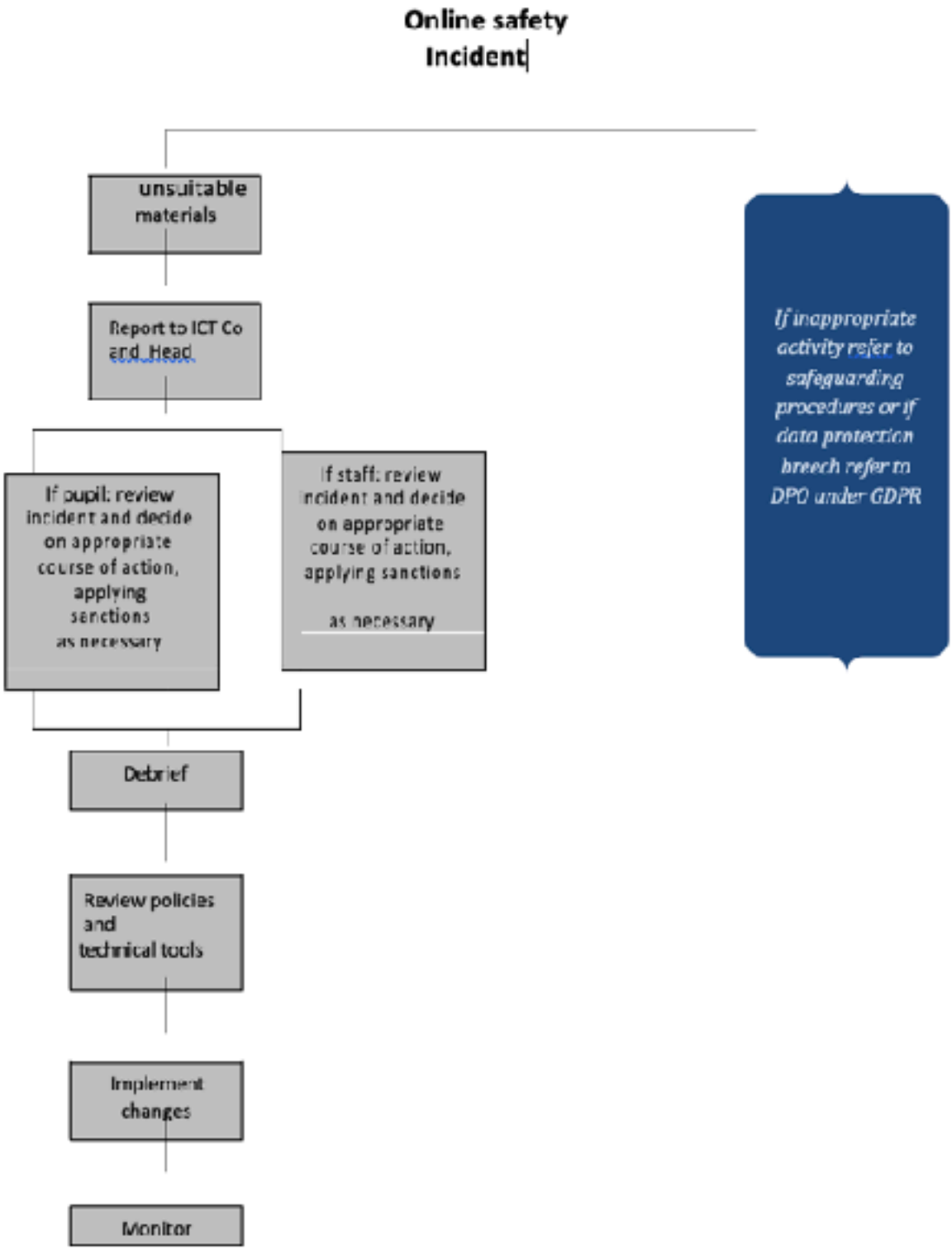
- All staff will be given the School Online safety Policy and its importance explained.
- All staff will be trained in Safeguarding procedures, including elements of Online safety and The Prevent Duty.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user. Discretion and professional conduct is essential.

Parents

- Parents' attention will be drawn to this and other relevant policies via the text system, website and newsletters. **The school will also organise Online safety workshops to support parents' how to best safeguard their children against potential online dangers.**

Updated October 2020
To be updated Summer 2023 @ PSP committee

Appendix A Flowchart for online safety incident



Appendix B

KS1 ONLINE SAFETY RULES

THINK THEN CLICK J

These rules help us to stay safe on the Internet

- We only use the internet when an adult is with us.
- We can click on the buttons or links when we know what they do.
- We can search the Internet with an adult.
- We always ask if we get lost on the Internet.
- We can send and open emails together.
- We can write polite and friendly emails to people that we know.

Appendix B

KS2 Online safety Rules

THINK THEN CLICK?

These rules help us to stay safe on the Internet

- We ask permission before using the internet.
- We only use websites that an adult has chosen.
- We tell an adult if we see anything we are uncomfortable with.
- We immediately close any webpage we are not sure about.
- We only email people an adult has approved.
- We send emails that are polite and friendly.
- We never give out personal information or passwords.
- We never arrange to meet anyone
- We do not open e-mails sent by anyone we
- We do not use internet chat rooms.

Appendix C

St. Luke's Acceptable use policy

Review date: Jan 2022

This policy outlines what are acceptable and unacceptable uses of ICT facilities within St. Luke's. It is relevant to pupils, staff, governors and visitors. Whilst we aim to support the full use of the vast educational potential of new technologies we also have a responsibility to provide safeguards against risk, unacceptable material and activities.
These guidelines are designed to protect pupils, staff and visitors from e-safety incidents and promote a safe e-learning environment for pupils.
At St. Luke's we believe that pupils should be trusted to use digital technologies in a principled and productive way. The general spirit of this policy is about giving everyone the opportunity to make productive decisions in the ways they decide to use digital technologies; we should all be fully engaged in the on-going debate about what responsible digital citizenship means and how we can nurture it within our school.

Examples of acceptable use are:

- Using web browsers to obtain information from the Internet
- Accessing databases for information as needed.
- Using e-mail for contacts.
- Using the school's network to promote the exchange of information to further education and research and is consistent with the mission of the school.
- Using the school's network to access outside resources that conform to this "Acceptable Use Policy".
- Using the network and Internet in a manner which respects the rights and property of others.
- Keeping all accounts and passwords confidential and inaccessible to others.
- Showing responsibility by making backup copies of material critical to you.
- Showing responsibility by taking precautions to prevent viruses on the school's equipment.
- Upon receipt of an attachment checking to making sure it is from a known source.
- Backing out of an accidentally encountered site that contains materials that violate the rules of acceptable use, and notifying a teacher or supervising adult of the occurrence immediately.
- Logging out or locking computers when they are left unattended
- Recognise that electronic communications sent through or stored on the school's network will be treated as school related and may be monitored or examined by the Headteacher or her/his authorised delegates for operational, maintenance, compliance, auditing, security and/or investigative purposes
- Reporting any damage to or loss of computer hardware immediately
- Saving documents onto appropriate storage areas of the school network or other appropriate storage systems

- Reporting any inappropriate behaviour and online bullying to the E-safety Coordinator
- Take reasonable care that there is no damage or loss of any equipment on loan from school
-

Examples of unacceptable use are:

- Use of the Internet for purposes that are illegal, unethical, harmful to the school, or non-productive.
- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Recording, filming or take photographs on school premises without permission and with consent of the parent or carer.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
- Relocating school information and communication equipment without prior permission
- Conducting a personal business using school resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Using inappropriate language: do not swear, use vulgarities or sexual innuendos.
- The sending of material likely to be offensive or objectionable to recipients.
- Using programs that harass school users or infiltrate a computing system and/or damage the software components is prohibited.
- Changing original software setting/configuration of school owned computers
- Doing harm to other people or their work.
- Do not install software on school computers unless authorised by the ICT Team.
- Doing damage to the computer or the network in any way.
- Interfering with the operation of the network by installing illegal software, shareware, or freeware.
- Plagiarisation and violation of copyright laws.
- Conversation in email using all upper case letters. This is considered shouting.
- Sharing your passwords with another person. Doing so could compromise the security of your files.
- Wasting limited resources such as disk space or printing capacity.
- Trespassing in another's folders, work, or files.
- Removing software CDs from their rightful location
- Giving out personal information such as your home address or telephone number. Use the school's address instead,
  but not the school's phone number.
- Downloading material from the Internet without specific authorisation from the ICT manager.
- Viewing, sending, or displaying offensive messages or pictures.
- Accessing sites that contain pornography; that spread hatred; that promote discrimination; that give instruction for acts
  of terrorism, harassment, murder, suicide, or other illegal activity.

I understand these guidelines and agree to follow them.

Full Name	
Signature	
Date	

Delete as appropriate

Staff	Pupil	Governor	Visitor

Appendix D

St. Luke's Primary School

ICT HOME USE CONSENT FORM

The purpose of this Consent form is to obtain permission and agreement from the Head Teacher to take school or school related ICT equipment for home use. Please note that this privilege may be revoked by the school at any time.

ICT EQUIPMENT FOR HOME USE

- Staff should charge iPad/Chromebook at home and bring them to school charged.
- Staff are allowed to connect their iPad/Chromebook to other WiFi networks but the school cannot provide any technical support in doing this. Connection to the internet should not be by wireless router unless the wireless connection signal is fully encrypted and password protected.
- Staff are responsible for providing any content filtering or restrictions on their own networks.
- The iPad/Chromebook is not to be loaned to anyone.

DAMAGE

- Occasionally, unexpected problems do occur with the iPad/Chromebook that is not the fault of the user (computer crashes, software errors, etc.). The school ICT team will assist staff with having these repaired. These issues will be remedied at no cost.
- Accidental Damage vs. Negligence. Accidents do happen. There is a difference, however, between an accident and negligence. The iPad/Chromebook warranty will cover normal wear and tear along with any defects that may arise during normal use of the device. Please note accidental damage to the screens on iPad/Chromebook is not covered by the warranty.
- After investigation by the school ICT team, if the iPad/Chromebook is deemed to be intentionally or negligently damaged by the member of staff, the member of staff may be subject to discipline and the cost of repair or replacement.

LOST AND STOLEN EQUIPMENT

- If any equipment is lost, the member of staff must report it to the Head Teacher (Matt Hipperson) or Office Manager (Shera Simpson) immediately.
- The circumstances of each situation involving lost equipment will be investigated individually.

- If any equipment is reported as stolen, a police report must be filed and a copy of the report must be provided to the school by the member of staff. If there is not clear evidence of theft, or the equipment has been lost due to staff negligence, the member of staff will be responsible for the full cost of replacing the item(s). This includes iPad/Chromebook and accessories.

FINANCIAL RESPONSIBILITY

- Outside of school hours, the iPad/Chromebook is not covered by the school's insurance policy. Any loss or damage will be the responsibility of the member of staff. The actual cost of replacement will be determined by Manufacturer but will not exceed the retail value of like-for-like replacement.

DECLARATION

I confirm that, as an authorised user of ST Luke's Primary Schools ICT facilities, I have read, understood and accepted all conditions in the ST Luke's ICT Home Use Consent Form.

Full Name	
Signature	
Date	

iPad/Chromebook Name:_____

Serial Number: _____

Head Teacher Signature: …….. **Date**:……/……../……

Appendix E

St. Luke's Guidance for the use of iPads, Chromebooks & laptops 2021 - 23

- iPads, Chromebooks & laptops are only for planned curricular work and are under **no circumstances** to be used at any other time in the

  day or for any leisure activities unless directed by teacher

- Children are to be monitored regularly every 5 mins when working on searches using these devices by the member of staff circulating the room

- The teacher is to explain to class that they will be checking the history tab and if the tab is cleared then the device will go to Mr Smythe to be checked

- Children are to understand that if they see/find any inappropriate images they must show the staff immediately and not show it to other children

- iPads, Chromebooks & laptops are to be stored and locked away as soon as session finished and keys given to school office.

Appendix F

The following Online Safety statements and guidelines help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a criminal offence to use a computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and all network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.