Learning Together for Life

Jesus said, 'Love one another as I have loved you'

John 15:12, New Testament ('Injil')

Stepney Greencoat

Church of England Primary School

Pupil Online Safety Policy

	By	Date
Policy Created	Marion Reilly	September 2018
Policy Approved	Governing Body	TBA
Policy Renewal Date		

Introduction to Online Safety for Pupils

Our Online Safety for Pupils Policy has been written by the school, building on examples and templates from the LGfL. The Policy is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance. It has been discussed with staff, agreed by the SLT and approved by Governors

Context and background

The technologies

Online tools and technologies have an all-encompassing role within the lives of children and adults and are enhancing communication and information sharing. We use a range of technology, apps and devices every day.

Our whole school approach to the safe use of ICT

In line with current statutory guidance (Keeping Children Safe in Education - Sept 2016) we ensure that we address the following key issues:

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subjected to harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm

We do this by making sure we have in place:

- An effective range of technological tools – eg content filters, monitoring software
- Appropriate policies and procedures, with clear roles and responsibilities
- A comprehensive Online Safety education programme for pupils, staff and parents

Roles and Responsibilities

Leadership team and Governors

Online Safety is recognised as an essential aspect of strategic leadership in this school and the Head, with the support of Governors, aims to embed safe practices into the culture of the school.
The SLT ensures that the Policy is implemented and compliance with the Policy is monitored.

Online Safety Co-ordinator

Our school Online Safety Co-ordinator is Marion Reilly. She keeps up to date with Online Safety issues and guidance and ensures the Head, senior management and Governors are updated as necessary.

School Staff

All teachers are responsible for promoting and supporting safe behaviours in their classrooms and following school Online Safety procedures. Central to this is fostering a 'No Blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials. Teachers must ensure all children are annually reminded of/sign: '*Rules for responsible ICT use for KS2 pupils*' document.
All staff should be familiar with other relevant policies including:

- Anti-Bullying policy
- GDPR Data Protection Policy
- Computing Curriculum Policy

Pupils

Pupils are expected to take an active part in planned lessons and activities to support their understanding and confidence in dealing with Online Safety issues, both at home and school. They are asked to agree to a set of guidelines and rules when using ICT at school: '*Rules for responsible ICT use for KS2 pupils'*. This document is to be revisited and signed annually.

Parents

Parents are given information about the school's Online Safety policy at the Admission interview. They are given copies of the pupil agreement for information and asked to support these rules with their children.

Technical and hardware guidance

School Internet provision
The school uses Virgin Media Business, as part of the London Grid for Learning Broadband consortium. Virgin provides an always-on broadband connection at speeds up to 100 MB.

Internet Content filter
The LGfL use a sophisticated content filter to ensure that as far as possible, only appropriate content from the Internet finds its way into school. Whilst this filtering technology is robust and generally effective at blocking unsuitable material, it is still possible for unsuitable material to occasionally get past the filter.

- All pupils and staff have been issued with clear guidelines on what to do if this happens, and parents will be informed where necessary.
- Pupils or staff who deliberately try and access unsuitable materials will be dealt with according to the rules outlined elsewhere in this document.

Classroom and user management
The school uses **Impero**, a network management and monitoring tool that reports any misuse or violation of the school's filtering strategy to the ICTCO

- Key words will trigger a report, and categories include Terrorism, Bullying, Gambling etc.
- The report is sent directly to the ICTCO and Technician
- Issues arising from this monitoring will be reported to the relevant SLT/Safeguarding staff member

Security and virus protection

The school subscribes to the LA/LGfL Antivirus software program, which uses Sophos and Norton Antivirus software. The software is monitored and updated regularly by the school technical support staff

- Any software messages or pop-up screens reporting evidence of viral infection should always be reported immediately to the ICTCO/ICT technician.

Supporting Parents and Families with Online Safety for pupils

- Online safety and pupil use of the Internet is discussed with parents at the admissions interview
- The school marks Safer Internet Day each year with class assemblies and parent workshops
- There is a section on the school website for Parents and families with useful links and resources.
- The school runs an Online Safety workshop for parents each year

Internet access at school

Access for all - Inclusion
All pupils have access to ICT as part of the curriculum. Details of how we manage access to the curriculum for all pupils is contained in our Inclusion Policy

Use of the Internet by pupils

- Pupils are always actively supervised by an adult when using the Internet
- Computers/tablets with Internet access are located so that screens can be seen at all times

ICT and Computing clubs

In line with our inclusion policies across the school, we want to ensure that all our pupils have access to the Internet, particularly where this will directly support their learning. To this end, we provide out of hours access and support in a lunch time drop in supervised ICT session (In Year groups): Mon to Fri 1.00 – 1.25 pm.

Out of Hours Provision

There will be no unsupervised access to the Internet at any time during Out of Hours provision.

Internet-enabled mobile phones and handheld devices

Young people have access to SMART mobile phones, tablets and music players. It is important that there are clear and enforceable rules for their use in school, particularly when they give access to the Internet.

- Pupils are not allowed to have personal mobile phones or other similar devices in school.
- Parents may request that phones are kept in the School office for pupils who need them on their journey
- Pupils are not allowed to take photographs using a camera phone or other camera of people or property on school premises unless given permission by a member of school staff.
- Pupils must under no circumstances upload pictures taken at school to a public website

Teaching the safe use of the Internet and ICT

The safe and responsible use of ICT is a statutory part of the Computing curriculum for all year groups from 1-6. The scheme of work that the school uses to teach Computing covers all aspects of the statutory online safety aspects of the curriculum. Lessons include online activities, discussion, written work, role play and presentations. The table below shows the key areas that will be taught to all pupils during their time at the school.
Please see the Computing and ICT Scheme of Work and Curriculum Policy for more details.

	Digital Literacy - Understanding and Using Technology Safely
Key Stage 1	• Know how computers and other devices can be connected into networks with cables and WiFi • Understand and describe some of the ways we communicate with others online • Be able to identify appropriate places to meet and chat online • To know why they should not to talk to strangers • Know what info they should NOT share with others online • Understand that there are rules about how we should use technology to keep us safe • Be able to discuss how they would ask for help if they felt they needed it
Lower Key Stage 2	• Know the basic structure of the Internet and World Wide Web and how information travels around it • Use digital communication tools (email, forums etc) safely and appropriately • Use a safe online social space (learning platform) to explore collaboration and networking • Know that there are copyright rules and that information should not be copied without permission • Know about the KIDSMART rules and other Online Safety portals • Understand that online communication should be responsible and appropriate • Describe how they would ask for help
Upper Key Stage 2	• Understand how information is named, organised, moved and stored on the Internet • Know about some of the key people and events in the history of computing and the Internet • Know about different online communication tools and some of the rules about use by young people • Be able to discuss issues around cyberbullying and appropriate online behaviour • Understand some of the issues around personal data and how it might be used by others if shared • Know that there are consequences to misusing digital information - eg plagiarism • Be able to explain how they would report concerns about online material or behaviours to the appropriate people

Resources

We use a range of resources, guidelines and materials offered by **LGfL, Espresso, Purple Mash**, **Kidsmart, Think U Know**, **Childnet** and **Common-Sense Media** as well as others.
Sharing contact details and information privacy
Pupils are taught that sharing personal information with others can be dangerous. They are taught to consider their Digital Footprint and how this might have consequences later in their lives

Information and Data Security

As specified elsewhere in this policy, pupil's personal details, identifying information, images or other sensitive details will never be used for any public Internet-based activity unless written permission has been obtained from a parent or legal guardian.
See the **GDPR Data Protection Policy** for more information on how we keep pupil data safe and secure.

Social Networking, Chat and Messaging

Online chat, discussion forums and social networking sites are increasingly popular with young people and can present a range of personal safety and privacy issues.
Pupils may become exposed to inappropriate material of a sexual, violent or extremist nature, and may come into contact with people who seek to 'groom' young people and encourage inappropriate, dangerous and in some cases illegal activities and behaviours.

- We use the resources, guidelines and materials offered by Kidsmart, Think U Know, Childnet and Common Sense Media as outlined above in the Safe Use of the Internet section to teach children how to use social networking and messaging/chat apps and tools safely and appropriately.
- Pupils are not allowed to use social networking sites in school and are reminded that such sites usually have age restrictions – 13 and older in most cases.
- Pupils may take part in discussion forums that teachers have evaluated as part of specific lesson activities. Individual pupil names or identifying information will never be used.

Internet Content

Suitable material
We encourage pupils to see the Internet as a rich and challenging resource, but we also recognise that it can be difficult to navigate and find useful and appropriate material.

- We provide pupils with suggestions for trusted and suitable sites across the curriculum
- staff always check the suitability of websites before using them in teaching
- We evaluate, purchase and provide access to relevant online digital resources libraries such as Espresso, Purple Mash
- Pupils and staff will not use Google image search as part of teaching and learning activities

Unsuitable material
Despite the best efforts of the LA and school staff, occasionally pupils may come cross something on the Internet that they find offensive, unpleasant or distressing. Pupils are taught to always report such experiences directly to an adult at the time they occur, so that action can be taken.
The action will include:

1. Logging the incident and making a note of the website and any other websites linked to it
2. Informing the ICTCO/Network manager and Head teacher
3. Informing the LA/Internet Service Provider so that the website can be added to the content filter
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future

Extremism

As part of other learning in Citizenship and PHSE children will be supported in making informed and appropriate choices if they encounter people and material online that may be challenging, prejudiced, inaccurate or that promote an extreme lifestyle or point of view. The school uses DfE guidelines and LA resources to support this

DfE PREVENT Duty

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

Educate against Hate (DfE/Home Office)

http://educateagainsthate.com/

Tower Hamlets Prevent Resources

http://www.towerhamlets.gov.uk/lgnl/education_and_learning/Prevent_resources/Support_for_Learning_Service_SLS_Prevent_Resources.aspx

Deliberate misuse of the Internet facilities

All pupils are asked to sign an Internet Use Agreement. (see example document)
Where a pupil is found to be using the Internet inappropriately, for example to download games, or search for unsuitable images, then sanctions will be applied according to the nature of the misuse, and any previous misuse.

Sanctions will include:

Unsuitable material (e.g. online games, celebrity pictures, music downloads, sport websites etc)

- Initial warning from class teacher
- Restriction of Internet access in school time
- Restriction of Internet access in school time
- Banning from out of school hours Internet facilities
- Letter to parent/carer
- Report to Head

Offensive material (e.g. pornographic images, racist, sexist or hate website or images etc)

- Incident logged and reported to Head
- Initial letter to parent/carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer
- Removal of Out of School Hours access to Internet
- Subsequent incidents will be treated very seriously by the Headteacher, and may result in exclusion and/or police involvement.

Cyberbullying - Online bullying and harassment

"Cyber bullying (also called 'online bullying') is when a person or a group of people uses the internet, email, online games or any other kind of digital technology to threaten, tease, upset or humiliate someone else."
Childline website

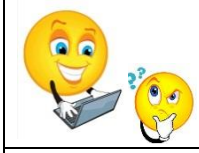
Cyber-bullying is an increasing issue for young people and can have a serious effect on pupils. Our school has a range of strategies and policies to help prevent online bullying, and support pupils and families if they are affected by it. These include:

- Pupils do not have access to social networking or chat websites or apps on school devices
- Pupils are taught how to use the Internet safely and responsibly
- Pupils and their families are given access to guidance and support resources from a variety of sources.
- Pupils can use Impero Confide to report any bullying issues in school to an appropriate adult

Please see our Anti Bullying Policy for more details on how we approach Cyber-Bullying at our school

Rules for responsible ICT use for KS1 pupils

Keep safe: Keep SMART

At School:	
	• I will always ask an adult before I use ICT equipment like a computer, laptop or camera
	• I will keep my username and password safe
	• I will make sure an adult is with me when I use the Internet
	• I will ask an adult if I don't know what to do
Outside School	
	• I know I should never share personal information like my name and address with anyone online
	• I know that if I see anything I don't like or understand I will tell an adult
	• I know I should be polite and kind to other people online

I agree to try and follow all these rules to keep me safe

Name: ……

Class: ……

Date: ……

Signature: ……

To be signed on admission and annually in the Autumn term.

Rules for responsible ICT use for KS2 pupils

Keep safe: Keep SMART

At school

- I will only use the school's computers and other electronic devices for schoolwork.
- I will use school ICT equipment and resources responsibly, and only when an adult is present.
- I will ask an adult if I am not sure what to do or how to use the resources.

- I will only edit or delete my own files and not look at, or change, other people's files.
- I will keep my logins and passwords secret and not share then with others

- I will not bring files into school (on a memory stick etc) without permission or upload inappropriate material to my school workspace.
- I will not use Google Image search to look for images online at school
- I will not use a personal mobile phone, personal computer or tablet in school.

- I will hand in any devices I need to use before or after school to the school office for safekeeping at the start of the school day and collect them at the end of the day.

Outside school

- I understand that I should 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 a trusted adult has given permission.

- I am aware that some websites and social networks have age restrictions (Facebook is for children 13 years and older) and I that should respect this.
- I understand that I should never arrange to meet someone I meet online unless my parent/carer has given me permission and I take a responsible adult with me.

- I understand that I should only send messages and e-mails to people that I know, or that a responsible adult has approved.
- I understand that any messages I send to others should be respectful

- I understand that cyberbullying is wrong and that I should talk to a trusted adult if it happens to me or I know it is happening to someone else.
- I know I should not open an attachment, or download a file, unless I know and trust the person who has sent it.
- If I see receive a message I do not like, I understand that I should not reply but I should keep the message and show it to a trusted adult as soon as possible

Name: ……

Class: …… **Date:** ……

Signature: ……

To be signed on admission and annually in the Autumn term.