



Pupil Online Safety Policy

Our Vision

We want Virginia Primary School to be a community of happy, confident, motivated lifelong learners. We want our children to be successful citizens who value themselves and each other. Therefore, we are continually striving to ensure that we nurture, challenge and enable each and every one to be the very best they can be in all areas of school life.

Rights Respecting School

We are a Right Respecting School and this policy supports the following articles from the United Nations on the Convention on the Rights of a Child:

- Article 17
- Article 19
- Article 36

Approved by:		Date:
Created on:	June 2018	Author: Marion Reilly
Last reviewed on:	October 2023	By: Marion Reilly
Next review due by:	October 2024	By: Marion Reilly

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 Coordinator is **Marion Reilly**. They keep 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 KS1/2 pupils'

All staff should be familiar with other relevant policies listed above.

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 annually to a set of guidelines and rules when using ICT at school: 'Rules for responsible ICT use for KS1/2 pupils'. This agreement is kept in their Computing book

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.

The school offers regular Parent Meetings to discuss issues around keeping children safe online

Other related policies and documents

The policy forms part of a suite of policies addressing the range of data protection and online safety issues that schools must address. These include:

- Data Protection and GDPR Policy
- ICT Security and Staff Acceptable Use Policy
- ICT and Computing Curriculum Policy
- Remote Learning Policy
- Safeguarding Policy
- Anti-Bullying Policy

Several government documents and policies have been consulted and embedded in this policy. These include:

- Keeping Children Safe in Education (DfE Sept 2019) Annex C Online Safety
- Computing Curriculum 2014
- Relationships and Health Education Curriculum 2020
- Education for a Connected World Framework 2020 Update (UKCCIS 2020)

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.

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

Out of Hours Provision

ICT and Computing clubs

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

Teaching the safe use of the Internet and ICT

The Computing Curriculum

The safe and responsible use of ICT is a statutory part of the Computing curriculum for all year groups. 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. *Please see the Computing and ICT scheme of work for more details.*

Health and Relationships Curriculum

Staying safe online and learning to use technologies to support wellbeing is now also an important part of the statutory Health and Relationships curriculum and will be taught as part of lessons in this area.

Resources

We use a range of resources, guidelines and materials offered by **LGfL**, **BBC Bitesize**, **Purple Mash**, **Kidsmart**, **Think U Know**, **Childnet**, **Google** and **Common-Sense Media** as well as others.

Pupil Accounts for Learning Platforms and Digital Resources

The school subscribes to several carefully chosen digital learning platforms and resource libraries and provides pupils with usernames and password where appropriate as they move through the school.

- These details will be supplied to pupils as and when they need them to log in. Some details will be shared across classes or groups and may be generic rather than individual to each pupil.
- Pupils will understand that all these accounts can be accessed and monitored by school staff, and anything they write or add to work or material stored in these platforms can be seen by staff.
- Pupils in KS2 may be provided with printed details of their username/password for these accounts. They will be expected to keep these details private unless asked by an adult to share the details to support access for a lesson or activity.

If individual pupil details are used to create accounts, then staff will ensure that this information is kept securely in line with GDPR regulations and Safeguarding procedures. Please see these policies for more information.

Pupil accounts will be deleted once the pupil leaves the school or no longer needs them, whichever is sooner.

Learning at Home Using Digital Resources

Accessing school digital resources outside school

If pupils are accessing digital resources from home, then their parents/carers will be informed in writing and will be expected to **return a signed form** to show that they understand the issues and responsibilities that are involved when their children are given access school resources outside school.

KS2 pupils will also be asked to sign a **Home Learning Agreement** that clarifies behaviour expectations and reminds them that school rules and procedures still apply when they use these tools and platforms outside school.

Remote Lessons/Live streaming/Video Conferencing

When pupils are involved in livestreamed lessons or video conferences with school staff there will be a **further agreement form** to be completed by the family and also a **Remote Classroom Agreement** to be completed by KS2 pupils setting out the rules and expected behaviour during a live-streamed lesson or conference.

See the Remote Learning Policy for more details.

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, using resources provided by <https://www.saferinternet.org.uk/>
- 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-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 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

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

Pupil's personal details, identifying information, images or other sensitive details will never be used for any public online 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 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.

- 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.
- We use the resources, guidelines and materials offered by Kidsmart, LGfL, 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.

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 suggesting them to children or using them in teaching.
- We evaluate, purchase and provide access to relevant online digital resources libraries
- 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 across something online 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/>

Lewisham/Southwark Prevent Programme

<https://lewisham.gov.uk/inmyarea/publicsafety/lewisham-prevent-programme>

<https://schools.southwark.gov.uk/safeguarding/prevent/educational-resources>

Deliberate misuse of the Internet facilities

All pupils are asked to sign an Internet Use Agreement. (see appendix) 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)

1. Initial warning from class teacher
2. Restriction of Internet access in school time
3. Banning from all school Internet facilities
4. Letter to parent/carer
5. Report to Head

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

1. Incident logged and reported to Head teacher
2. Initial letter to parent/carer
3. Removal of Internet privileges/username etc
4. Meeting with Parent/Carer to re-sign Internet use agreement
5. Removal of Out of School Hours access to Internet
6. 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.

No Blame Approach

Sometimes children are part of cyberbullying without realising. There can be a lot of pressure from other children to "join in" and it is difficult to stop once you are part of it.




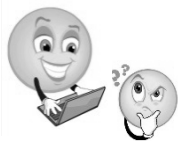



School staff employ a 'no blame' approach to support and encourage pupils to tell an adult if they know that someone is being bullied online, or if they feel that they have become involved themselves in cyber-bullying. We encourage pupils and parents to discuss any concerns or worries they have about online bullying both in school and out of school with staff. All concerns are taken seriously and dealt with appropriately. Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school child protection procedures.



Virginia Primary School

Using ICT Safely and Responsibly for KS1 pupils

Keep safe: Keep SMART

At school and outside school:	
	I will always ask an adult before I use ICT equipment like a computer, tablet, robot, laptop or camera.
	I will keep my usernames and passwords safe, and not share it with anyone other than an adult that I know and trust.
	I will make sure an adult is with me when I use the Internet on a computer or any other device.
	I will ask an adult for help if I don't know what to do or see something that I don't like or understand online.
	I will treat all school ICT equipment carefully and tell an adult if it goes wrong.
	I will never share personal and private information like my name and address with anyone online.
	I will be polite and kind to other people online.
I agree to try and follow all these rules to keep me safe	

Please sign below at the start of each school year to show you understand these rules.

Name:			
Year group	Class	Signature	Date
Reception			
Year 1			
Year 2			



Virginia Primary School

Safe and Responsible ICT use for KS2 pupils



Keep safe: Keep SMART

At School - rules

- I will only use the school's computers and electronic devices for school work.
- I will use school ICT equipment and resources responsibly, and only when an adult is present.
- I will use any online learning accounts set up for me by the school responsibly.
- I will keep my logins and passwords secret and not share them with others.
- 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 not upload personal files to any school network or digital device without permission.
- I will not use Google Image search to look for images online at school.
- I will not use any personal electronic devices in school without permission
- I will follow school rules about personal devices that I need to use before and after school



Outside school - guidelines

- I understand that I should not share personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.
- 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 know that I should respect by any age limits and restrictions on websites and apps that I use.
- I know I should not open a message attachment or file unless I trust the sender.
- I understand that I should only send messages and e-mails to people that I know and trust.
- I understand that any messages I send to others should be respectful, truthful and kind.
- If I see receive a message I do not like, I know that I should not reply but I should keep the message and show it to a trusted adult as soon as possible.
- I know that cyberbullying is wrong and that I should talk to a trusted adult if it happens to me.
- I know that I should also talk to a trusted adult if I think someone else is being cyberbullied.



Please sign below at the start of each year to show you understand these rules and guidelines

Name:			
Year group	Class	Signature	Date
Year 3			
Year 4			
Year 5			
Year 6			