



# 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

**Policy Updated: October 2017**

**Policy Renewal frequency: Annual**

**Policy Renewal Date: September 2018**

## Rationale

Our Online Safety Policy has been written by the school, building on The London Grid for Learning (LGfL) Exemplar Policy and other example policies and documents.

- *This Policy is drawn up to protect all parties: the students, the staff and the school and aims to provide clear advice and guidance on how to minimise risks and deal with any infringements*
- *It has been discussed with staff, agreed by the senior management and approved by Governors*

## Context and background

### The technologies

ICT in the 21<sup>st</sup> Century has an all-encompassing role within the lives of children and adults. New internet and online technologies are enhancing communication and the sharing of information, and we use a range of technology, apps, devices and every day.

### Young people have access to the Internet on many different devices and types of technology:

- Computers and laptops
- iPads and tablet PCs
- Mobile phones and smart phones – *iPhone, Galaxy 7*
- Some TVs and DVD players
- Game Consoles – *X-Box, Wii, PlayStation,*
- Hand-Held game devices - *Nintendo DS*
- Voice activated 'smart assistants' - *Amazon Alexa*

### Young people enjoy many different activities online:

- Watching and sharing videos - *You Tube, Facebook Live*
- Talking to friends, sharing videos, links and photos - *What's App*
- Posting about what they are doing/eating/wearing etc – *Facebook, Instagram*
- Posting messages and comments - *Twitter, Tumblr,*
- Sharing favourite websites and images - *Pinterest*
- Taking and sharing photos and comments - *Instagram*
- Playing online games with other people – *Miniclip, Xbox, PlayStation*
- Video calling – *Skype, Facetime*
- Searching for pictures and information - *Google*
- Sharing music tracks and comments - *Musical.ly*

## Our whole school approach to the safe use of ICT

**In line with current statutory guidance (Keeping Children Safe in Education - 5<sup>th</sup> 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

*For more information on the school policy for the teaching and learning of Computing and ICT, please see the Computing and ICT Curriculum Policy.*

## Roles and Responsibilities

### Leadership team

The SLT ensures that the Policy is implemented and compliance with the Policy is monitored. 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.

### Online Safety Co-ordinator

Our school Online Safety Co-ordinator is **Marion Reilly**. S/he keeps up to date with Online Safety issues and guidance. The school's Online Safety coordinator ensures the Head, senior management and Governors are updated as necessary.

### Governors

Governors need to have an overview understanding of Online Safety issues and strategies at this school. We ensure our governors are aware of our local and national guidance on Online Safety and are updated at least annually on policy developments.

### 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.

### All staff should be familiar with the schools' Policies including:

- The Staff role in providing Online Safety education for pupils
- Cyberbullying procedures
- Safe use of the school network, equipment and data
- Appropriate publication of pupil information/photographs and use of website

### Staff INSET

Staff are reminded / updated about Online Safety matters at least once a year, and have INSET when appropriate

### 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

### 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.

## 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, clubs etc

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

## Technical Provision and Equipment

### 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*

### Downloading files and applications

- *Pupils and staff are not allowed to download and install any material from the Internet unless directed to do so by an appropriate 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.*

## Teaching the safe use of the Internet and ICT

The safe and responsible use of ICT is now a statutory part of the Computing curriculum introduced in September 2014, and will be taught discretely with age appropriate lessons, activities and resources.

We teach pupils to use the Internet as a resource for learning and information and as a way to communicate.

*Please see the Computing and ICT scheme of work for more details.*

### Using the Internet for as a resource for learning

The Internet is an invaluable resource for learning for all our pupils, and we use it across the curriculum both for researching information and a source of digital learning materials.

We teach all of our pupils how to find appropriate information on the Internet, and how to ensure as far as possible that they understand who has made this information available, and how accurate and truthful it is.

*More details can be found in our Computing and ICT Curriculum Policy.*

Teachers carefully plan all Internet-based teaching to ensure that pupils are focused and using appropriate and relevant materials. Children are taught:

- *How to use search engines and how to evaluate Internet-based information*
- *How to investigate the possible authors of web-based materials.*
- *How to carry out simple checks for bias and misinformation*

### Using e-Mail at school

We teach the responsible and safe use of e-mail as part of our Computing curriculum

- *Where necessary, pupils are provided with a school e-mail address via the London Grid for Learning Safe Mail system, which is secure and designed for use by pupils. Staff can monitor this account*

## **Social Networking and Online Chat**

Social media in a variety of forms is used with increasing frequency by pupils out of school, and can also contribute to learning across a range of curriculum areas. However they can present a range of personal safety and privacy issues for young people, and there have been some serious cases highlighted in the media.

Pupils may become exposed to inappropriate material and may come into contact with people who seek to 'groom' young people and encourage inappropriate, dangerous and in some cases illegal activities/behaviours.

Pupils have lessons each term covering a wide range of aspects of this area of technology

- *Pupils are not allowed to use social networking sites or apps 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, 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.*

## **Use of Social Media by the school**

The school has a Twitter account that is used to share news and photos on a regular basis. The Twitter account is administered by a trained member of staff in accordance with this policy

## **Cyber-bullying**

(from NSPCC website: <https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/bullying-and-cyberbullying/what-is-bullying-cyberbullying>)

Cyber-bullying is an increasingly common form of bullying behaviour which happens on social networks, games and mobile phones. Cyber-bullying can include spreading rumours about someone, or posting nasty or embarrassing messages, images or videos.

Children may know who's bullying them online – it may be an extension of offline peer bullying - or they may be targeted by someone using a fake or anonymous account. It's easy to be anonymous online and this may increase the likelihood of engaging in bullying behaviour.

### **Cyber-bullying includes:**

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- 'trolling' - the sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations

### **Dealing with cyber-bullying incidents**

The school generally treats cyber-bullying incidents in the same way as other bullying incidents as outlined in the Anti-Bullying Policy. Some strategies specific to cyber-bullying include:

- Parents are contacted if an incident comes to light as it is usually happening out of school.
- The school will invite parents in to discuss ways that they can support their children to overcome bullying
- The school will offer support to parents in dealing with pupils who are involved with cyber-bullying

Please see the following safeguarding policies for more information

- Positive Behaviour Policy
- Anti-Bullying Policy
- Safeguarding Policy

## Online 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.

- *Where possible, and particularly with younger children, we provide pupils with suggestions for suitable sites across the curriculum, and staff always check the suitability of websites before using them*
- *We evaluate, purchase and provide access to relevant online digital resources libraries - These include **Discovery Espresso** and **Purple Mash***

### ***Unsuitable material***

Despite the best efforts of the LA and school staff, occasionally pupils may come across 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
- 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](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 KS1 and KS2 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
- 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 teacher
- Initial letter to parent/carer
- Removal of Internet privileges/username etc
- Meeting with Parent/Carer to re-sign Internet use agreement
- 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.

## Digital Imaging

We recognise that taking and using digital images at school can enhance learning and encourage parental engagement by celebrating school activities and pupil success. We also recognise that new technology developments mean that photos and videos can be taken, shared and uploaded to public online spaces much more easily, and great care needs to be taken to ensure that safeguarding and data protection guidelines are followed stringently. The safety of children is our highest priority. To support this the following are in place.

### Taking and use of digital images by school staff

- Digital images of pupils are only taken to support teaching and learning
- Staff will not take photos or videos of pupils in any non-learning situation, 1:1 or otherwise
- Staff are not allowed to take digital images of pupils on their own cameras or mobile devices
- Images of pupils will be stored safely and securely according to the Data Protection policy
- Staff sign the school's Acceptable Use Policy and this includes a clause on the use of mobile phones/personal equipment for taking pictures of pupils;

### School Use of photos/videos of pupils

- 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 (or annually).;
- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials/DVDs;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term, high profile use

### Taking and use of digital images by parents/carers

Parents/carers are allowed to take photographs of school events with the following conditions:

- Photos can only be taken in the event venue as advised by school staff
- Photos are strictly for personal use only
- Photos that contain images of other children cannot be shared on social media or other public online spaces – breach of this condition will result in a ban on further use of cameras in school
- Video recording of pupils or staff is not allowed on school premises
- Parents/carers must stop taking images if asked to do so by a staff member

### Taking and use of digital images by pupils

- Pupils will only take digital images as part of a learning activity
- Pupils will always be supervised by an adult when taking and working with digital images
- Pupils will only take digital images using approved school equipment

### Teaching pupils about safe use of digital images outside school

- Pupils are taught about how images can be manipulated in their online safety education programme and also taught to consider how to publish for a wide range of audiences which might include governors, parents or younger children as part of their computing scheme of work;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

### Images on the School Website and Social Media accounts

- Please see the School Website policy for information on this aspect of digital imaging

# Virginia Primary 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: .....

# Virginia Primary School

## Rules for responsible ICT use for KS2 pupils



### 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 them 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: .....



# Use of the Internet and ICT resources by school staff

## ***The Internet***

The Internet is a valuable resource for school staff with a wealth of resources, teaching materials and information. It allows staff to share resources with other schools, and to engage in discussion.

We are committed to encouraging and supporting our school staff to make the best use of the Internet and all the opportunities it offers to enhance our teaching and support learning.

## ***Internet Availability***

- The Internet is available in school to all staff for professional use. The school also provides an LGfL user account that gives further access to specific resources and online tools.

## ***Professional use***

- Staff are expected to model appropriate ICT and Internet use at all times. This supports our commitment to encouraging safe and appropriate ICT and Internet use by our pupils
- Staff also consider inclusion and equalities issues when using ICT and the Internet, and to provide pupils with appropriate models to support the school Inclusion and Equal Opportunities policies.
- Staff who need support or INSET in using ICT as part of their professional practice can ask for support from the ICT Co-ordinator.

## ***Personal use of the Internet and ICT resources***

- We recognise that staff may occasionally find it useful to use the Internet at work for personal purposes
- However, all staff must be aware of the school policy on using school Internet and ICT resources for personal use. These are outlined in the staff agreement form below

## ***E-mail***

- Staff members will be given a school e-mail address and we ask staff to use it for all professional communication with colleagues, organisations, companies and other groups.
- Staff are reminded that using this e-mail address means that they are representing the school, and all communications must reflect this.

## ***Online discussion groups, bulletin boards and forums, online chat and messaging***

- The use of online discussion groups and bulletin boards relating to professional practice and continuing professional development is encouraged, staff are reminded that they are representing the school, and appropriate professional standards should apply to all postings and messages.

## ***Social Networking***

- The school appreciates that many staff will use social networking sites and tools.
- The use of social networking tools and how it relates to the professional life of school staff is covered in Staff Professional Conduct expectations and agreements.
- There are resources, weblinks and guidance in the Online Safety folder on the Staff Drive.

## ***Data Protection and Copyright***

- The school has data protection policy in place – please see Data Protection policy for more details.
- Staff are aware of this policy, and how it relates to Internet and ICT use, in particular with regard to pupil data and photographs, and follow the guidelines as necessary.
- Staff understand that there are complex copyright issues around many online resources and materials, and always give appropriate credit when using online materials or resources in teaching and learning materials. They also support pupils to do the same.

# School Staff Online Safety Agreement Form

This document covers the use of school digital technologies and networks in and out of school.

## **Access**

- I will obtain the appropriate log on details and passwords from the ICT Co-ordinator.
- I will not reveal my password(s) to anyone other than the appropriate staff managing the system.
- If my password is compromised, I will ensure I change it.
- I will not use anyone else's password if they reveal it to me.
- I will not allow unauthorised individuals to access school ICT systems or resources.

## **Appropriate Use**

- 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 never view, upload, download or send any material which is likely to be unsuitable for children or material that could be considered offensive to colleagues. This applies to any material of a violent, dangerous or inappropriate sexual content.
- I will not download, use or upload any material which is copyright, does not have the appropriate licensing or that might compromise the network.
- I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the Online Safety coordinator or member of the SMT.

## **Professional Conduct** (See Code of Conduct document Section 8 for more details)

- I will not engage in any online activity that may compromise my professional responsibilities.
- I will ensure that any private social networking sites / blogs etc that I create or actively contribute to are not confused with my professional role.
- I will never include pupils or former pupils as part of a non-professional social network or group.
- I will ensure that I represent the school in a professional and appropriate way online
- 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 appropriate line manager / school named contact.

## **Email**

- I will only use the approved, secure email system for any school business or communication with parents
- I will not communicate with pupils by email unless using approved school email accounts as part of approved school work.

## **Photographs and Video**

- I will not use personal digital cameras or camera phones for taking and transferring images of pupils or staff without permission and will not store images at home without permission.
- I will never associate pupil names or personal information with images or videos published in school publications or on the Internet (in accordance with school policy and parental guidance).

## **Personal Use**

- I understand that I may use Internet facilities for personal use at lunchtimes, break times and before and after school, where computers are not being used for educational purposes.
- I understand that I may access private e-mail accounts during the availability periods outlined above for personal use, but will not download any attachments, pictures or other material onto school computers, or onto the school network area.
- I understand that the forwarding of e-mail chain letters, inappropriate 'jokes' etc is forbidden.
- I will not use the school Internet facilities for personal access to public discussion groups or bulletin boards chat rooms or Instant Messaging.

### ***Use of School Equipment out of school***

- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any “significant personal use” as defined by HM Revenue and Customs.
- I will keep any ‘loaned’ equipment up-to-date, using the school’s recommended anti-virus, firewall and will return it when requested to be updated by the school technician.
- I will not connect a computer/laptop/device to the network that does not have anti-virus software.

### ***Teaching and Learning***

- I will always actively supervise, or arrange for suitable adult supervision of pupils that I have directed or allowed to use the Internet.
- I will embed the school’s Online Safety curriculum into my teaching, using agreed resources and materials.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will only use the Internet for professional purposes when pupils are present in an ICT suite, or a classroom with Internet access.

### ***Copyright***

- I will not publish or distribute work that is protected by copyright.
- I will teach pupils to reference online resources when they use them in a report or publication.

### ***Data protection***

- I will not give out or share personal addresses (including email), telephone / fax numbers of any adult or students (including myself) working at the school.
- I will not take pupil data, photographs or video from the school premises without the full permission of the head teacher e.g. on a laptop, memory stick or any other removable media.
- I will ensure any confidential data that I wish to transport from one location to another is protected by encryption and that I follow school data security protocols when using any such data at any location.
- I will respect the privacy of other users’ data, and will never enter the file areas of other staff without their express permission.
- 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.

## **User Signature**

- I agree to abide by all the points above.
- I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the school’s most recent Online Safety policies.
- I wish to have an email account, be connected to the Internet via the school network and be able to use the school’s ICT resources and systems.

Signature ..... Date .....

Full Name ..... (printed)

Job title .....

School .....

### **Authorised Signature (Head Teacher)**

I approve this user to be set-up.

Signature ..... Date .....

Full Name ..... (printed)