



# *Blue Gate Fields Junior School*

## **Pupil Online Safety Policy**

### **Policy details:**

- **Date of policy:** April 2018
- **Last updated:** May 2022, May 2023
- **Date of next review:** May 2024

**Person (s) responsible for implementation and monitoring:**  
Sian Acreman (Head Teacher)

**Signature (Head teacher)**

**Signature (Chair of governors)**

### **Links to other policies:**

- Staff ICT Security Agreement and Policy
- Safeguarding Children Policy
- Anti-Bullying Policy
- Online Safety and School Closure: Safeguarding for Online Home Learning Policy

## 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 Mark Cooke. He 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
- Staff ICT Security Policy and Staff Agreement

### 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 200 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 currently 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*

\*We are, however, moving towards **Senso Cloud** in the Summer/Autumn term 2022 for our device management and monitoring.

## 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, 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 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

We currently do not have ICT and Computing clubs.

## 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 or social media

## 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 for more details.*

	<b>Digital Literacy - Understanding and Using Technology Safely</b>
<b>Lower Key Stage 2</b>	<ul style="list-style-type: none"><li>• Know the basic structure of the Internet and World Wide Web and how information travels around it</li><li>• Use digital communication tools (email, forums etc) safely and appropriately</li><li>• Use a safe online social space (learning platform) to explore collaboration and networking</li><li>• Know that there are copyright rules and that information should not be copied without permission</li><li>• Know about the KIDSMART rules and other Online Safety portals</li><li>• Understand that online communication should be responsible and appropriate</li><li>• Describe how they would ask for help</li></ul>
<b>Upper Key Stage 2</b>	<ul style="list-style-type: none"><li>• Understand how information is named, organised, moved and stored on the Internet</li><li>• Know about some of the key people and events in the history of computing and the Internet</li><li>• Know about different online communication tools and some of the rules about use by young people</li><li>• Be able to discuss issues around cyberbullying and appropriate online behaviour</li><li>• Understand some of the issues around personal data and how it might be used by others if shared</li><li>• Know that there are consequences to misusing digital information - eg plagiarism</li><li>• Be able to explain how they would report concerns about online material or behaviours to the appropriate people</li></ul>

## 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 suggesting them to children or using them in teaching.
- We evaluate, purchase and provide access to relevant online digital resources libraries including Discovery Espresso and 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 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
4. Discussion with the pupil about the incident, and how to avoid similar experiences in future
5. Teaching pupils to use **Impero Confide**- a desktop shortcut that will allow users to report any issues, directly to an appropriate member of staff

## 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/ignl/education\\_and\\_learning/Prevent\\_resources/Support\\_for\\_Learning\\_Service\\_SLS\\_Prevent\\_Resources.aspx](http://www.towerhamlets.gov.uk/ignl/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
- 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.

## 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

### 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 activity.

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.

## Online Safety and School Closure: Appendix on Safeguarding for Online Home Learning

The Corona Virus Pandemic and subsequent government directions on self-isolation and school closures are having a huge impact on schools and education. Schools are introducing new ways of working to support the continuing education and pastoral support of school pupils during the school closure period, which may continue over the whole of the summer term.

Some of this support will use ICT and online learning systems and resources, both in school, and at staff and pupil's homes. This is unprecedented and requires a re-evaluation of current Online Safety policy alongside the wider safeguarding issues that home-based learning presents.

Pupils and families will be spending much more time online on a range of devices including computers, laptops, mobile phones, tablets, game consoles, smart TVs etc. They will be accessing new websites, communication tools and apps, learning sites, online discussion groups and forums, and may be inundated with information and requests to learn new online skills, behaviours and attitudes.

Staff will be expected to learn new skills and teaching strategies in a very short space of time, and will be delivering lessons to children in an entirely new way, without face-to face contact or feedback.

To support safeguarding in this areas School leaders will be:

- Keeping up to date with Government guidance and directives in this area.
- Making use of National and local guidance for accredited and approved organisations e.g. LGfL.
- Keeping Governors informed of developments, strategies and new safeguarding arrangements.

The situation relating to online safety and home learning falls into four broad areas:

1. Ensuring pupils and families have access to advice and guidance about online safety for home learning.
2. Ensuring that the school is providing appropriate and secure online learning tools and systems for staff.
3. Ensuring staff are teaching pupils how to use online learning resources and communication tools safely.
4. Ensuring staff are maintaining professional standards and upholding safeguarding and online safety policies.

## **Pupil Online Safety Policy Appendix**

### **What staff are doing to teach pupils how to use online learning and communication tools safely**

- Reminding pupils of the online safety learning they have already done at school.
- Modelling good online safety behaviour when communicating with pupils online.
- Ensuring that Online Safety lessons and activities are a key part of any Home Learning timetable or plan.
- Using an updated Pupil Online Safety Agreement to highlight good online safety rules and strategies.
- Providing links for pupils to access appropriate resources, games and activities that support Online Safety, including new resources created for the current situation.
- Monitoring pupil activity on school-provided online learning platforms to ensure appropriate behaviour.
- Addressing any issues with pupils overstepping professional boundaries immediately, with guidance for parents if necessary and reporting back to SLT.

### **What the school is doing to give families access to guidance about online safety for home learning**

- Making sure the school's Online Safety posters and key messages are displayed on the school website, and on materials that are sent home.
- Alerting and directing parents and families to suitable materials and resources that will help them support their children to be safe online, either by email, on the school website or by post.
- Making sure parents know about the school platforms and resources that their children will be accessing.
- Keeping parents informed of national news and advice, including information about online scams and fraud.
- Providing staff with support and INSET where needed to develop the skills to provide Online learning.
- Disseminating up to date information from Government and other organisations to staff.
- Ensuring staff feel able to raise issues and concerns about new ways of working with SLT.



# Blue Gate Fields Junior School



## Rules for Responsible use of Technology

### Stay Safe Stay SMART

#### At School

- 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 platform 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 without permission
- I will not use Google Image search to look for images online at 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.
- I will not use any personal electronic devices in school without permission.

#### Home Learning

- I will send my home learning work and any questions to my year group email address or my Google Classroom.
- I will remember to write my name on my work when I email it to my teachers.
- I will tell a trusted adult if I see or hear anything inappropriate when online.

<b>Name:</b>			
<b>Year group</b>	<b>Class</b>	<b>Signature</b>	<b>Date</b>
<b>Year 3</b>			
<b>Year 4</b>			
<b>Year 5</b>			
<b>Year 6</b>			