Blue Gate Fields

Junior School

Staff ICT Security Policy and Staff Agreement

Policy details:

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

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

S E Acreman

Signature (Chair of governors)

Robert Oakley

Links to other policies:

- Pupil Online Safety Policy
- Safeguarding Children Policy
- Personal Mobile Devices & Digital Cameras in School Policy
- Online Safety and School Closure: Safeguarding for Online Home Learning Policy
- Code of Conduct For Staff, Governors, Volunteers and Visitors
- GDPR Policy

Introduction to Information Communication Technology (ICT) Security

Blue Gate Fields Junior School is committed to preserving the confidentiality, integrity and availability of all the electronic information assets throughout the school. This is critical to the on-going functioning and good governance of the school.

Information Communication Technology (ICT)

Information Communication Technologies encompass a range of devices, platforms and systems that store, process and share information and data. They can include:

- Computers and laptops
- Server-based networks
- Mobile devices (tablets, phones, ebook readers))
- CCTV Cameras
- Removable storage devices
- Digital cameras
- Sound recording devices
- Learning platforms and digital library resources
- Cloud-based platforms and networks
- Cloud-based applications and

This ICT Security Policy outlines the school's approach to electronic information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the school's electronic information systems.
The school is committed to a robust implementation of ICT Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its electronic data. The principles defined in this policy will be applied to all of the electronic information assets for which the school is responsible.

Roles and Responsibilities

ICT Security 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.

Senior Leadership Team (SLT)

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

ICT Security Manager

Our school ICT Security Manager is Mark Cooke
They keep up to date with Information Security issues and guidance and ensures the SLT are updated

Governors

The Governing Body has a responsibility to ensure that the ICT Security Policy is updated and monitored regularly. We ensure our governors are aware of local and national guidance on ICT Security and are updated regularly.

School Staff

All school staff are required to understand the policies relating to ICT Security, and the rules and restrictions that are part of the agreement that they sign each year

Parents

The Information Security policy is available to parents on the school website, and a printed copy can be requested

Other Related Polices

The ICT Security 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
- Pupil Online Safety Policy
- ICT and Computing Curriculum Policy

Internet Access

School Internet Provision

The school uses Virgin Media Business, as part of the London Grid for Learning (LGfL) 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 in the **Pupil Online Safety Policy**

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 by any user (staff and pupil) to the ICT Security Manager

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

Downloading Files and Applications

Pupils should not download/install any material from the Internet onto any school device or system.
Staff can only download resources/materials that are for professional use onto school devices and networks

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 Technical Support Service and/or ICT Security Manager

Connection of personal staff devices/external agency devices to the Internet

On occasion a staff member or an external party (eg School Nurse) will need to connect an eternal device to the school Internet service. The school has a secure guest Internet access account for this purpose. Access information is available from the school office.
This Internet access can be monitored and should only be used for professional purposes unless agreed with SLT.

The School Network

The school has a sever based network with staff-only and shared drives. Staff are given access according to the school's **ICT Access Control guidelines** – see below.
The server is accessed through laptops and computer work stations in classrooms, offices and meeting rooms around the school. Only authorised Technical Support Services staff have access to the server itself and are able to change settings and profiles etc.

ICT Access Control

Access to school ICT systems for new staff users is authorised by SLT and then provided by the authorised Technical Support Services. Network settings ensure that passwords are suitably complex and are updated regularly in line with best practice and the GDPR.

Access management

A database of staff users, their access rights and credentials is kept securely in line with GDPR Regulations by the Technical Support Officer and can be reviewed when necessary by SLT
Staff access is automatically terminated when they leave the employment of the school.

The following accounts might be provided, depending on staff responsibilities:

- A **school network** username and password for access to the school server network
- An **LGfL Unique Sign On (USO**) account which acts as their official staff email account (via LGfL StaffMail) and also gives access to LGfL resources and tools
- A **school Google Education** username and password which gives access to the school Google Resources and shared/team drives
- An **RM Integris** account for access to the web based registration system
- An account for **Medical Tracker** to support the tracking of pupils with medical needs

Restricted Access

Some users are granted access to restricted areas of the network or cloud-based storage on the basis of their roles and responsibilities as agreed with SLT. These credentials must be kept private and secure and not shared with other staff members.

Remote Access

The school provides access to some areas of the school network remotely using **Home Access Plus**. This allows staff to log in to the school network from outside school to retrieve documents and files. Files may be downloaded for editing and then re-uploaded to the school server. Staff may also access cloud-based storage and information systems outside school

Any school files containing personal information downloaded to personal computers, tablets, phones or tablets for editing should be deleted from these devices immediately in line with the GDP Regulations and Data Protection Policy.

Remote access to school systems is restricted to those specified staff who need access and removed immediately when a staff member leaves the school.

Cloud Based Services

The school subscribes to several approved cloud-based services that provide tools, storage and applications for both staff and pupil use. The accounts for staff include:

- A **Purple Mash Staff account** which gives access to the school Purple Mash Learning Tools suite
- An **Espresso staff account** which gives access to the staff area of the Espresso Digital Library
- **Mathletics Staff Accounts** to allow management of pupil Mathletics accounts
- **Active Learn** staff accounts to support Active Learn pupil support resources
- **Hamilton Trust** resources staff accounts
- **Tig Tag** staff accounts for science resources
- **Testbase** accounts to enable access to SATS papers
- **Do My Reports** for staff to access the Do My Reports website
- **Educare** account for staff training

Staff also have access to several third party online resources via generic school accounts. These include CLPE, Nicholas Roberts Reading Resources, Oxford Owl etc
Staff accounts for these services are controlled in the same way as other access to ICT services

Visitors

All visitors (including supply staff and contractors) to the school will be made aware of the general safeguarding arrangements of the school on arrival, and the key elements of the staff ICT Security Agreement as it relates to their visit.

- Access to the school network and Internet services on any device will not be given unless set up and supervised by an appropriate school staff member who has full knowledge of the ICT Security Policy.
- Visitors will not have access to online devices unless agreed by the Senior Leadership Team, and for a defined purpose related to their visit. (eg the school nurse may need to access the guest Wi-Fi password to allow access to materials and resources relevant to the visit)
- Visitors will not be permitted to take any photos or make digital video or sound recordings of school activities or resources unless specifically agreed beforehand with the Senior Management Team.
- Visitors agree to abide by professional standards in the dealings with the school, and to maintain these standards outside school once the visit has ended. This includes social media and other online platforms
- Visitors agree that personal mobile phones and other digital devices must be kept out of sight and switched to silent mode in the presence of pupils and parents

Supply/Temporary teaching staff

Short Term Supply staff will not be given their own access to the Internet and network. They will be given access by a generic **supply staff user account** that has restricted access to the school network.

Documents stored in the My Documents area of this account will be deleted and the password changed regularly Access to other systems and cloud-based services will be given on an individual basis as the need arises, according to the discretion of the ICT Security Manager/Senior Management Team.

Supply staff will be given a printed summary of this policy as part of the **Supply Teacher and Visitor Information Sheet** and asked to sign the **Supply Staff ICT Security Agreement** when they arrive at school.

School Mobile Devices

School staff may use a selection of mobile ICT devices to support teaching and learning and to ensure the safety of pupils and staff. They may be used in school and outside school when authorized by SLT.
These currently include:

- **Staff iPads**
- **Class Digital Cameras**

All of these devices are managed by the school and have appropriate restrictions and security features enabled. They are regularly checked and updated by the Technical Support Services. Use of these devices is monitored by the ICT Security Manager and they are signed in and out by staff via the school office administrator
They are not used in any circumstances for staff personal business.
Please see the **Personal Mobile Devices & Digital Cameras in School Policy** for more details

Disposal of ICT Equipment with data storage

All school equipment that may contain information or data will be disposed of using an approved Third-Party Company that will provide a certificate of disposal. See the **Data Protection Policy** for more information.

Use of the Internet and ICT resources by school staff

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.

E-mail accounts

- Staff members will be given a school e-mail address (which is also their LGfL USO account) and should use it for all professional communications
- 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 forums **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
- The personal use of these services is forbidden on school premises or on school equipment

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

Personal Devices in schools

Staff may bring in their own devices to school on occasion.

- They are not allowed to connect these devices to the school network without permission from the SLT and this connection must by initially set up by Technical Support Services if agreed.
- Mobile phones and other personal devices must NOT be used in the presence of pupils, parents or while staff are engaged in professional activities (eg in a staff meeting) unless previously arranged with SLT.

Use of Personal Devices to capture digital media

The use of personal devices to capture or record digital images, sound or video is not permitted unless agreed beforehand with the ICT Security Manager and/or the Senior Management Team. If permission is given, then any images, sounds or videos should be deleted completely from the device once transferred to the school network or data storage.
Loaned equipment must only be used for professional purposes, both in and out of school.
Please see the **Personal Mobile Devices & Digital Cameras in School Policy** for more details

GDPR, Data Protection and Copyright

- Please see the **GDPR and Data Protection Policy** for more details on how we approach data protection
- 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 materials. They also support pupils to do the same.

Staff Laptop and ICT Equipment Loans

Some equipment is available for loan to staff, with permission from the ICT Security Manager and Headteacher. The appropriate forms and agreements must be signed. Loaned equipment must only be used for professional purposes, both in and out of school.

- Any member of staff who borrows or uses a school laptop, computer or any other ICT equipment or device must adhere to all aspects of this ICT Security Policy.
- This must be the case wherever the laptop, computer or other such device is being used as it remains the property of **Blue Gate Fields Junior School** at all times.
- Staff must undertake to take proper care of the equipment whilst in their possession and will abide by the requirements of the school's insurance policy with regard to protecting the equipment from loss or damage. They must also agree that, should the equipment be lost or damaged due to exposure to a non-insured risk, they will replace or arrange for the repair of the equipment at their own expense.

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.

ICT Security Policy and Staff Agreement Appendix

What the school is doing to provide appropriate and secure online learning tools and systems for staff

- Ensuring all platforms and online communication tools used to communicate with pupils are secure, appropriate and are part of a robust school managed system.
- Liaising with technical support staff to ensure robust security for remote access to school network resources and online learning tools, including the secure management of staff and pupil accounts and passwords.
- Being clear about learning intentions and pastoral support objectives for all online learning activities.
- Providing clear and explicit rules, boundaries and expectations for all online learning experiences set up and managed by school staff – e.g. Purple Mash Learning Blogs, responses to Home Learning.
- Ensuring staff and pupils know the difference between material that is public (e.g. on the school website), shared with school pupils (a class blog) and private between a pupil and their teachers (email responses to the google year group collaborative inboxes year3/4/5/6@bgfjs.org, a 2Do comment).

What staff are doing to ensure the online learning they deliver is safe, appropriate and professional

- Only using systems provided or agreed by the school to communicate with pupils and families i.e. when responding to pupils' home learning work use the collaborative year group inboxes.
- Remembering to be particularly careful about posting images of children with identifying information, especially if the photo was taken at the pupil's home.
- Ensuring that any devices logged in to school remote learning or cloud-based resources are supervised and logged off when not being used.
- Ensuring that all pupil data and information stored on their personal devices (with permission from the school) is deleted as soon as it is no longer needed.
- Ensuring they are up to date with all relevant school policies, and asking for clarification if necessary.
- Taking up offers of support and training on using new systems and tools.
- Sharing their own expertise and experience with colleagues to support staff development.

Staff Communication with Children

School staff should:

- not seek to communicate/make contact or respond to contact with pupils outside of the purposes of their work.
- not give out their personal details.
- use only the equipment and internet services/platforms provided by the school or setting, unless school policies state otherwise.
- only use internet-enabled personal devices in line with school acceptable use policies.
- follow their school / setting's acceptable use policy and online safety guidance.
- ensure that their use of technologies could not bring their employer into disrepute.
- not discuss or share data relating to children/ parents / carers in staff social media groups.

Staff Dress and Appearance

School staff should wear clothing which:

- promotes a positive and professional image.
- is appropriate to their role.
- is not likely to be viewed as offensive.
- does not distract, cause embarrassment or give rise to misunderstanding.
- is absent of any political or otherwise contentious slogans.
- is not considered to be discriminatory.
- is compliant with professional standards.

Staff and Families: Social contact outside of the workplace

School staff should:

- always approve any planned social contact with pupils or parents with senior colleagues, for example when it is part of a reward scheme.
- advise senior management of any regular social contact they have with a pupil which could give rise to concern.
- refrain from sending personal communication to pupils or parents unless agreed with senior managers.
- inform senior management of any relationship with a parent where this extends beyond the usual parent/professional relationship.
- inform senior management of any requests or arrangements where parents wish to use their services outside of the workplace e.g. babysitting, tutoring.

School Staff ICT Security Acceptable Use Agreement Form

Blue Gate Fields Junior School

Online Safety Policy: School Staff Agreement Form

This document covers the use of school digital technologies and networks in and out of school.
Updated April 2020

Access

- I will obtain the appropriate log on details and passwords from the **ICT technician (Dan)**.
- I will not reveal my password(s) to anyone other than the persons responsible for running and maintaining 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 Safety coordinator or member of the SMT.

Professional Conduct

- 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 ensure that my activities on social media do not breach professional conduct standards (see Teacher Standards – Professional Conduct section).
- 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 when sending e-mail, contributing to online discussion or posting to public websites using school facilities.
- 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 (currently: LGfL Staff Mail and **gmail - @bgfjs.org**).
- I will not communicate with pupils by email unless using approved school email accounts as part of approved school work. **When responding to pupils' home learning work I will use the collaborative year group inboxes.**

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 available and 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 ICT technician.
- I will not connect a computer, laptop or other device to the network that does not have up-to-date 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 e-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 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.

Home Learning protection

- **I will use the collaborative year group inboxes to communicate and respond to pupils' work. I will not communicate with pupils by personal emails. I Know I can contact the school ICT technician if unsure.**
- **If recording videos/video lessons (including taking still photographs) I will film in a neutral area where nothing personal or inappropriate can be seen or heard in the background. Additionally, I will ensure I am dressed in accordance with the *Staff Dress and Appearance* section in the *Appendix on Safeguarding for Online Home Learning* found in the *Staff ICT Security Policy and Staff Agreement.***
- **I will not conduct livestreaming lessons.**
- **I will only use school online/video sharing accounts to support lessons and home learning blogs, e.g. The school Vimeo account. I will not use personal accounts.**

- **When communicating with children via email/collaborative year group inbox, I will be conscious of safeguarding issues around sending and receiving messages and pictures.**
- **I will use all of the same awareness and professionalism as if I am working in school. I will immediately contact the Designated Safeguard Lead (Sian, Jo or Patricia) if I have any concerns regarding safeguarding.**
- **I will make sure not to leave sensitive pupil information unattended whilst working from home.**
- **I will make sure I do not leave work emails and blog editing pages unattended whilst working from home.**

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 **and safeguarding** 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 …………………………………………………………………….. Job title…………………………….

Agreement for access provision
I approve this user to have access to the school network and Internet provision as outlined below:

School Network Account		SLT Access to restricted areas		Access to restricted SEND areas	
LGfL USO/Staff mail account		Purple Mash Staff Account		Espresso Staff Account	
Other:		Other:		Other:	

Authorised Signature (Head Teacher)

Signature .... Date

Full Name .... (printed)