BURLINGTON JUNIOR SCHOOL

Acceptable Usage Policy

Written By	**Senior staff**	
Frequency of Review	**3 years**	
Date reviewed and approved by Governing Body	**July 2020**	
Date of next review	**July 2024**	
Display on Website	✓	
Purpose	This policy ensures staff are clear about how to use and store data responsibly and for ensuring pupils are safe when using the internet.	
Consultation	**Governors**	**x**
	Parents	**x**
	Pupils	**x**
	Staff	✓
Links with other policies	**Prevent Radicalisation**	

Introduction
These three policy statements have been created to protect the interests of the school its staff, pupils and Governors. These conditions may be changed at the discretion of the Headteacher at any time.

All staff and Governors wishing to use school Computing resources and systems need to sign a copy of the declaration contained in this document and return to the Headteacher, where it will be kept on file. If there are any concerns, access rights will be withdrawn. A record will be maintained of all users with system access. Users will be removed from this record when access is no longer required, in accordance with the Data Protection Act. Users will be advised of any changes made to these policies.

POLICY STATEMENT 1 – Acceptable Use
The Computing facilities are owned by the school (this includes laptops allocated to individual staff) and their use is an entitlement for all authorised users, subject to the conditions set out below:

- All Computing based activity must be appropriate to a school environment
- Access to shared resources must be made via the user's authorised account and password
- Users will not disclose their account name and password to any other person
- Users will always log in using their own usernames and passwords
- It is forbidden to partake in any activity that threatens the integrity of the school's facilities, including the use of the internet to access inappropriate materials
- The school reserves the right to monitor the use of Computing resources, emails sent or received, files held and internet sites visited at any time, including examining and deleting any files held.
- Users must prepare the use of video clips and images to ensure they are appropriate before sharing with children
- Staff must always log off or lock any computer after use
- No staff or governors are allowed to use their own devices (Bring Your Own Devices BYOD) to access school data. This includes phones, iPads and laptops

By logging on to the school's Computing resources all users agree to abide by the condition above and agree not to use them to:

- Access chat room services or download files from internet without express permission
- Publish information which could identify the user or any other person directly on any web page
- Send or receive any material that is obscene or defamatory or which is intended to annoy, harass or intimidate another person.
- Upload, download or otherwise transmit commercial software or any copyrighted materials
- Introduce any form of computer virus into the network
- Transmit unsolicited commercial or advertising material
- Use the service to set up or run a personal business
- Post anonymous messages or send chain letters
- Broadcast unsolicited personal views on social, political or religious matters
- Represent personal opinions as those of the school or Local Authority
- Send pupil or staff data through unauthorised lockdowns

All users also agree to:

- Seek permission from the Headteacher or Subject Leader for Computing before downloading any software such as itunes/Spotify etc.
- Report any inadvertent access to inappropriate websites

POLICY STATEMENT 2 - Transfer of Sensitive Data (GDPR)

We aim to produce guidelines for staff to minimise a breach of data during which sensitive data may be lost, become vulnerable, altered or stolen. Sensitive data is defined as any personal or confidential information that can be linked to a specific person.

With regards to sensitive data staff are expected to:

- Never create or store data which contains any client-specific information on personal devices, regardless of where they intend to use the data
- Only use password protected school supplied laptops or memory sticks should they need to transport sensitive data
- Only use approved cloud storage for sensitive data: MyDrive/USO FX2 on LGFL.net
- Only use laptops and memory sticks as a means of transporting data on a temporary basis
- Transport data to school storage facility and delete data from laptop or memory stick as soon as it is no longer needed
- Only take sensitive physical data (e.g. pupil file) home when absolutely necessary and with the express permission of the Headteacher
- Never leave sensitive data/files unattended
- Maintain the confidential nature of the data wherever that data may be e.g. car/home
- Never read or make notes on sensitive files during a journey on public transport (no labels visible)
- Never post images relating to school on internet or social networking
- Access to data is restricted to those for whom it is a requirement of their role.

With regards to email staff are expected to be aware that:

- The content security and safe receipt of information sent by email is always the responsibility of the sender
- Emails can be the subject of interception
- Good practice includes the use of initials rather than names, dates of birth, addresses etc.
- Normal non-secure email may be used for day-to-day communication with colleagues, third parties and other agencies where the nature of the information is not confidential
- Any electronic communication between staff at school and the Local Authority which contains sensitive data is made using a secure system called USO-FX or between Encrypted LGFL mail accounts.
- Anonymised information may be sent through normal email only when extra care has been taken to verify the recipient (e.g. telephone call)
- Pupil specific reports and documents should not be sent as an attachment to an email to anyone outside the Local Authority
- Emails should always be of a professional nature with due regard to the recipient
- Emails containing sensitive data and/or in connection with school matters should only be created by an appropriate member of staff.
- Sensitive data must only be sent via Atomwide by an appropriate member of staff.

Data Breaches

On the discovery of a potential breach of data the matter should be referred immediately to the Headteacher. The Headteacher will then initiate an enquiry to ascertain the nature and scope of the breach. If it is believed that sensitive data may have been compromised then the Headteacher will notify the Local Authority or Information Commissioner's Office (ICO) and seek advice regarding subsequent action.

POLICY STATEMENT 3 – Online safety

Online Safety for pupils

All adults within the school are responsible for ensuring pupils are safe when using the internet. Teaching staff are required to teach Online Safety for half a term in every year group.

In addition to Online Safety, teachers will discuss and explain the LGFL 12 rules for responsible Computing Use poster to ever class (Appendix 1). Pupils from Year 3 upwards are asked to sign a copy of the Code of Conduct at the beginning of each academic year in their school diaries. A copy of the code is displayed in the Computing Suite.

POLICY STATEMENT 4 – Remote learning

When the school has adopted remote learning in place of teaching in the classroom, adults will be required to use school devices and learning platforms safely and appropriately.

With regards to remote learning staff are expected to:

- Use school owned devices at home in the same way they would be used in school.
- When signing in to the school Google account, appropriate websites are visited and sign-ins to external sites are authorised by the computing coordinator, Headteacher or deputy Headteacher.
- Seek prior approval for livestreaming with an individual pupil or class from the Headteacher. This can only take place in on school premises where it can be recorded (for safeguarding pupils and staff) to the server so that it is not stored on a personal or portable device. Use the LGFL '20 safeguarding considerations for lesson livestreaming' if it this has been approved.
- Quickly pass safeguarding issues to DSL
- Only privately message pupils in regards to their work, their general well-being and maintain a professional relationship with pupils.
- Direct parent messages to parent@bjs.rbksch.org and not reply via a learning platform.
- Monitor the learning platform regularly.

Online Safety for adults

In addition to the Acceptable Use and Transfer of Data policies, staff are required to use the Computing facilities sensibly, lawfully and professionally. Training in online safety will be provided at regular intervals for all staff by AfC ICT and online safety advisor (Peter Cowley).

****

Acceptable Usage Policy for staff

With reference to Burlington Junior School's Computing Policy statements covering:

- Acceptable Use
- Transfer of Data
- Online Safety

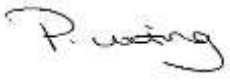
I confirm I have read the policy statements noted above and agree to abide by the conditions.

I understand that misuse of schools Computing equipment or systems is a serious offence and could lead to disciplinary procedures.

User's Name _____

User's signature_____

Headteacher's signature



Date September 2020

Appendix 1

Keeping safe: stop, think, before you click!

12 rules for responsible ICT use

These rules will keep everyone safe and help us to be fair to others.

- I will only use the school's computers for schoolwork and homework.
- I will only edit or delete my own files and not look at, or change, other people's files without their permission.
- I will keep my logins and passwords secret.
- I will not bring files into school without permission or upload inappropriate material to my workspace.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I will not attempt to visit Internet sites that I know to be banned by the school.
- I will only e-mail people I know, or a responsible adult has approved.
- The messages I send, or information I upload, will always be polite and sensible.
- I will not open an attachment, or download a file, unless I know and trust the person who has sent it.
- I will 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 will never arrange to meet someone I have only ever previously met on the Internet, unless my parent/carer has given me permission and I take a responsible adult with me.
- If I see anything I am unhappy with or I receive a message I do not like, I will not respond to it but I will show a teacher / responsible adult.


Don't share...
- Your family name (first name is OK)
- Family details like address, phone number etc
- Emails, IDs and passwords
- Your photo or what you look like
- Your School name