



Acceptable Usage Policy

Written By	Senior staff	
Frequency of Review	Annually	
Date reviewed and approved by Governing Body	Autumn 2026	
Date of next review	Autumn 2027	
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 GDPR/data protection Online safety Safeguarding	

Introduction

These 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 the [declaration](#) which is sent out by the school office annually. If there are any concerns, access rights will be withdrawn.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 .
- 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
- Only use laptops and memory sticks as a means of transporting data on a temporary basis
- Only transport data to school storage facility on the school cloud
- Never take sensitive physical data off site (e.g. pupil file)
- Never leave sensitive data/files unattended
- Never post images relating to school on internet or socials
- 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 Egress
- 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 and sent securely.

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. We use Satswana for our GDPR support.

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 read and sign the pupil acceptable usage agreement each September.

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 school accounts, appropriate websites are visited and sign-ins to external sites are authorised by the computing lead, 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.
- Quickly pass safeguarding issues to DSL
- Only message pupils in regards to their work, their general well-being and maintain a professional relationship with pupils on an agreed platform ie Google classroom.
- Direct parent messages to parent@burlingtonjunior.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.

All staff complete cyber security training annually.