BUCKINGHAM
PRIMARY SCHOOL

ICT Acceptable Use Policy (AUP)

Safety and Responsibilities Policy

Staff

Version: 1.01 Release date: August 2023 Review date: August 2024
Authorised by: DPO
Location: Shared policy, please contact gdpr@turniton.co.uk

turn IT on
Connecting schools and technology

Contents

1. Equipment
2. Internet and Email
3. External services
4. Privacy and data protection
5. Service availability
6. Use of digital images and photographing
7. Roles and responsibilities
8. Entitlement
9. Data breach management

ICT Acceptable Use Policy :

Safety and Responsibilities Policy – Staff

The staff at Buckingham Primary School strongly believes in the educational value of ICT and recognises its potential to support the curriculum. Every effort will be made to provide high quality experiences to students using the ICT system, however, inappropriate and / or illegal interaction with any service or system is strictly prohibited.

This Information & Communication Technology (ICT) policy is set within the framework of the aims and curriculum principles of the school.

The overall aim for Information and Communication Technology is to enrich learning for all students and to ensure that teachers develop confidence and competence to use Information and Communication Technology in the effective teaching of their subject.

Vision

The school recognises the importance of Information Technology in the school curriculum both as a way to develop skills and concepts in their own right and as a way of enriching, enhancing and extending the delivery of all subjects across the curriculum. It also recognises that school leavers need certain 'key skills' for further study and employment, some of which relate to using ICT.

Aims of this document

The school's aims with regard to ICT set out below are to develop:

- Communication - through reading and selecting from a range of sources, planning, writing and refining texts in different styles and for different purposes, communicating face-to-face and by e-mail, and discussing and reflecting critically on their own and on others' work
- Application of number - through working with quantitative data and mathematical models
- Thinking skills - through helping students to identify relevant sources of information, develop ideas and work collaboratively to solve problems
- Enterprise and entrepreneurial skills - through encouraging students to design and implement solutions to real problems
- Work-related learning - through providing students with access to a wide range of ICT applications and methodologies
- Education for sustainable development - through developing students' understanding of the implications of ICT for working life, society and the environment
- Learning and performance - through reviewing, modifying and evaluating their work as it progresses
- good Health and Safety attitudes and practice

Listed below are the terms of this agreement. All Staff at Buckingham Primary School are expected to use the ICT systems in accordance with these terms. Violation of terms outlined in this document may lead to loss of access and / or disciplinary action.

Please read this document carefully and sign and date it to indicate your acceptance of the terms herein. Access to the college ICT system will only be enabled once this document has been signed.

1. Equipment

1.1 Vandalism

Vandalism is defined as any action that harms or damages any equipment or data. This includes, but is not limited to:

- Deliberate damage to computer hardware such as monitors, base units, printers, keyboards, mice or other hardware.
- Modification or removal of software
- Unauthorised modification of data
- Unauthorised configuration changes
- Creation or uploading or computer viruses or other malware
- Deliberate deletion of files

Any of these actions reduce the availability and reliability of computer equipment, puts other users' data at risk and increases downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements that may benefit other users. Increased maintenance costs incurred by repairs undertaken to damaged equipment also reduces the funds that can be spent on improvements to the system.

1.2 Use of Removable Storage Media

The only removable storage devices and media that Staff should use on the school's ICT equipment and network is equipment that has been purchased by Buckingham Primary School.

All removable media must be authorised and offer data security options like encryption to safeguard data. The general guidance is staff should not use USB storage devices for school work and data storage. The school offer remote access which connect to the school network, this is the preferred solutions to remove the need for USB storage, the remote access system and cloud system like Google's G-Suite and Microsoft's Office 365 are also available to help transfer data securely. Please talk to our ICT Coordinator for more information.

Removable media includes but is not restricted to:

- CDs / DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- MP3 Players
- Digital Cameras
- Bluetooth device
- Webcams
- Backup tapes or drives
- Personal cloud storage platforms

The school has obligations under Freedom of Information and Data Protection legislation to control the use of removable media (including security and retention). Therefore, only school issued removable media devices must be used to store school information and data.
Staff should **NOT** use personal removable media to transfer school data to any other location.

1.3 Printers and Consumables

Printers are provided across the school for use by staff and should use the printers sparingly and for educational purposes only. Printing of non-education or offensive material is strongly prohibited. All staff should note that all printer use is recorded and monitored.

- Always print documents in mono unless colour is essential
- Proof-read your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink, toner or paper.
- Avoid printing directly from the Internet where possible. Internet pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.

1.3.1 Printer Accounting

Software can used to monitor and report printer usage. Papercut or similar can be used for viewing all network printer and their usage. Papercut or a similar program may be used to quota user printer usage as per user policies based on credits.

1.3.2 Secure printing

Secure printing allows printing by requiring the user to have access to the printer via an authentication method to collect print jobs from the printing device. Authentication methods include pin codes, finger prints and swipe cards.

1.4 Data Security and Retention

All data stored on Buckingham Primary School network is backed up daily and backups are stored for up to [2 weeks]. If you accidentally delete a file or files in your folder, then inform a member of ICT staff immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than [2 weeks] previously.

All school data is controlled via data retention guidelines and all staff should check with their Data Protection Lead or Data Protection Officer before deleting any school information.

2. Internet and Email

2.1 Content Filtering

Buckingham Primary School provides two layers of internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. The use of Internet and email is a privilege and inappropriate use may result in disciplinary action.

2.2 Acceptable use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws.
- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.

- Do not access Internet chat sites. These represent a significant security threat to both students and the college network. Remember that people you may meet on such a chat site are not always who they seem.
- Never reveal or enter any personal information into a website, especially the home addresses, personal telephone numbers or passwords of yourself, other staff members or students.
- The use of on-line games is prohibited. These consume valuable network resources that could be used by others to benefit their studies. Remember that Internet access in college is provided for educational and research purposes only.
- Do not print out pages directly from a website. Web pages are often not suitably formatted for printing and this may cause significant wastage of paper. If you wish to use content from websites, consider using the copy and paste facility to move it into a Word or Publisher document.
- Within lessons, the Internet should only be used to access material related to the work currently being done.
- Do not attempt to download or install software from the Internet. Deliberate modification of computer configuration amounts to vandalism and as such is strictly prohibited. All software and online resources must be checked, and all suppliers are checked for suitability under data protection regulations.
- Do not use the Internet to order goods or services from on-line e-commerce or auction sites.
- It is forbidden for students to subscribe to any newsletter, catalogue or other form of correspondence via the Internet, regardless of its nature.
- The use of on-line mailing lists, newsgroups or web forums, except any provided by Buckingham Primary School. Staff are reminded that ALL Internet access is logged and actively monitored. Internet access logs are stored for up to twelve months and usage reports can and will be provided to any member of school staff upon request.

2.3 Email

Staff are provided with an email address by the school. Email may be used for any legitimate educational or research activity. Staff should use email in accordance with the following guidelines and are reminded that email communications may be monitored at any time. Staff are expected to use email in a responsible manner. The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but it not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be taken in all cases.

- Be Polite - never send or encourage others to send abusive messages
- Use appropriate language - remember that you are a representative of the school on a global public system. What you say and do can be viewed by others. Never swear, use vulgarities or any other inappropriate language. Illegal activities of any kind are strictly forbidden
- Do not reveal any personal information about yourself or anyone else, especially home addresses, personal telephone numbers, usernames or passwords. Remember that electronic mail is not guaranteed to be private
- Messages relating to, or in support of any illegal activities may be reported to the authorities
- Whilst it is possible to attach files to an email message, students are advised that email is not generally suited to transferring large files. Whilst there are no hard and fast rules regarding file sizes that can be attached to an email message, files exceeding approximately 20MB in size are generally considered to be excessively large and students should consider using other methods to transfer such files
- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the school network
  If any of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law, we reserve

- All emails sent from Buckingham Primary School email accounts must include the official school email disclaimer. The email disclaimer should be attached automatically but the email system
- Staff should not use the email system as a file storage area and all-important files should be stored on the school's network or shared cloud storage locations. Staff accounts may be removed on termination of employment and important data may be lost.
- Staff email accounts may be archived for up to 12 months before they are removed from the email system
- Staff should not forward emails to personal email accounts
- Staff should make sure they mask email addresses of recipients for external emails. If the email contains multiple recipients, you should use the BCC field for all recipients

2.4 Cloud storage provided via school email systems

Cloud storage platforms are now common place and you should consider where you store data at all times. Staff should not use the email system to store sensitive school information and data. All data should be stored in appropriate storage areas for example shared folders on the school network or in the cloud. Please consult your school ICT coordinator or ICT Support provider for information on correct storage procedures.

- Email based cloud storage folders will be removed when your emails account is removed from the system and this data may be needed by the school
- Staff should not use personal cloud storage services for school data. Platforms like Dropbox and personal versions of Google's G-Drive and Microsoft's OneDrive are not GDPR compliant. School versions of these platforms are GDPR compliant and should be the default for school data storage

3. External Services

Buckingham Primary School provides several services that are accessible externally, using any device with an Internet connection. These should be used strictly for educational activities only and in accordance with the following guidelines.

3.1 Web-Email

Web email provides remote access to your email account from home or any location with an Internet connection. Use of this service is subject to the following guidelines. Use of the service is closely and actively monitored and any abuse or mis-use will result in this service being withdrawn and / or other disciplinary action being taken.

- Web-email is provided for use of Buckingham Primary School staff and students. Access by any other party is strictly prohibited
- By using Web-Email, you signify that you are a student or employee of Buckingham Primary School and that you have been authorised to use the system by the relevant school authority
- Always Observe security guidelines. Never reveal your password to anyone
- Remember to treat file attachments with caution. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the computer from which you are working. Do not download or open file attachments unless you are certain of both their content and origin. Buckingham Primary School accepts no responsibility for damage caused to any external equipment or software as a result of using the web-email service

4. Privacy and Data Protection

4.1 Passwords

- Never reveal your password to anyone else or ask others for their password.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.
- Password should be a minimum of 8 characters in length
- If you forget your password, inform a member of ICT Support staff immediately.
- If you believe that someone else may have discovered your password, then change it immediately and inform ICT Support

4.2 Security

- Never attempt to access files or programs to which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.
- You should report any security concerns immediately to senior management and ICT support
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action
- If personal devices are used to access school systems, they must be password protected or PIN/Finger recognition/Face recognition for mobile devices
- All personal devices are used to access school systems must have all data erased and be factory reset before sale or disposal

4.3 Web based teaching resources

- All web hosted teaching resources where the school share personal or sensitive information must be vetted and assessed as a data processor under the GDPR legislation, for example if you input student names for login information or synchronise information via an automated process
- All software and teaching resources should be checked and authorised by our school data protection lead.

5. Service Availability

Buckingham Primary School makes no warranties of any kind whether expressed or implied for the ICT services it is providing. Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the school will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the school ICT system is at your own risk. Buckingham Primary School specifically denies any responsibility for the accuracy of information obtained whilst using the ICT systems. In addition, Buckingham Primary School cannot make any guarantees as to the availability of services delivered via the ICT system, such as the school website, email, or any other remote access system.

6. Use of digital images and photographing

6.1. In Buckingham Primary School:

- A member of the admin team takes overall editorial responsibility to ensure that the website content is accurate, and quality of presentation is maintained

- Uploading of information is restricted to the website the designated admin staff member and the Headteacher
- The school web site complies with the school's guidelines for publications
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status
- The point of contact on the web site is the school address and telephone number. Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached and will be published in line with guidance from the DFE and data protection regulations
- 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. All staff much check before using images of students for publications to make sure consent has been gained
- Digital images /video of pupils are stored in the teachers' shared images folder on the network and images are deleted at the end of the year – unless an item is specifically kept for a key school publication
- We do not use pupils' names when saving images in the file names or in the <ALT> tags when publishing to the school website
- We do not include the full names of pupils in the credits of any published school produced video materials / DVDs / video uploads
- Staff must not use personal devices to record video or photos, Staff should only use school cameras and devices to take pictures and videos of students

6.2. Social networking and personal publishing

- The schools will block/filter access to social networking sites
- Newsgroups will be blocked unless specific use is approved
- Staff will be advised never to give out personal details of any kind which may identify them and / or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests and clubs etc
- Staff are advised not to place personal photos on any social network space. They should consider how public the information is and consider using private areas. Staff should be aware around background detail in a photograph which could identify their location e.g. house number, street name or school etc
- Teachers' official blogs or wikis should be password protected and run from the school website. Teachers should be advised not to run social network spaces for student use on a personal basis
- Pupils should be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others
- Staff should not publish specific and detailed private thoughts
- Staff should be aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments

7. Roles and Responsibilities

The roles and responsibilities will be split between the senior management team, the ICT Committee, the subject leader and the network manager as follows: -

7.1 SLT will be responsible for: -

- managing the implementation of the ICT policy across all departments
- ensuring staff access to ICT
- liaison with feeder and/or receiving schools
- monitoring the curriculum
- health and safety policy and practice
- reviewing the ICT policy
- Data protection and the GDPR

7.2 The Computing Team will be responsible for: -

- developing a strategic overview of ICT across the school
- developing the school's ICT policy
- providing a formal channel for discussion and communication between the SLT and the Computing Lead and the Network Manager. Hence the membership of the Computing team shall consist of, *ex officio*, the Headteacher , the Assistant Headteacher (Curriculum), the Computing lead, the Computing network team and the Chairman of the Governors' Curriculum Sub-Committee.
- making recommendations to the SLT about the allocation of funds to ICT, including an assessment of departmental ICT development bids

7.3 The Computing lead and AHT will be responsible for: -

- assessment of pupils in ICT
- meeting statutory requirements
- curriculum development within ICT
- updating the scheme of work
- identifying the ICT support needed by staff
- arranging in-service support
- attending appropriate courses to update knowledge of current developments
- maintaining links with the Advisory Team for ICT
- ensuring continuity between year groups
- ensuring ICT progression
- contributing to the School Improvement Plan on an annual basis

7.4 Other subject leaders / Computing lead will be responsible for: -

- ensuring that sufficient opportunities are provided in their subject areas for students to apply and develop their ICT skills
- ensuring these opportunities are identified in the departmental schemes of work
- in consultation with the Head of ICT, ensuring that progression in ICT skills is reflected in schemes of work
- identifying ICT support needed by staff in their departments
- in consultation with the Head of ICT, arranging appropriate in-service training in ICT
- identifying in their annual departmental development plans the on-going ICT needs of their departments

7.5 Computing Lead and AHT, will be responsible for: -

- purchasing/organising ICT resources
- maintaining records of software licences and their deployment
- making sure all staff understand system for logging faults and use of the Internet/email
- Reporting of network issues to ICT Support helpdesk.
- Overseeing equipment maintenance and ensuring staff make visiting technician aware of any faults that may arise via fault reporting system.
- keep staff abreast of new developments
- liaise with external support technician and helpdesk

7.6 External support team. (ICT Support, MIS Support, Finance Support etc)

- liaise with the Computing lead
- maintaining the managing the internet connection supplied by contract.
- maintaining and supplying email service
- maintaining classroom equipment
- Advise school of any issues that may arise from visits and solutions.
- keep school abreast of any new technology that may help staff in educating pupils.

- looking for solutions for existing problems as they arise

7.7. Staff and Pupils

- all users to use any equipment responsibly
- report any faults found to the appropriate person and put fault in the correct log to get repaired if required

8. Entitlement

This section covers classroom and shared resource equipment

8.1. All classrooms will have a networked PC connected to a working IWB. In addition to the programmes of study provision is made for staff and students to use ICT equipment at staff digression during lunch and dinner breaks as well as after school clubs.

8.2. Any laptops, cameras or associated equipment will only leave the school premise with the express consent of the head teacher or designated member of staff with the following provisos.

8.2.1 Short loan

Short term loans are determined as overnight or for a weekend and will be required to be signed out with designated member of staff.

- All loan equipment is recorded with serial number and member of staff's details
- the equipment is available for school use during normal school term time hours
- any damage or failure is reported as soon as the equipment is return
- all laptops will be loaned out with a suitable carry case and necessary charging units

8.2.2 Extended loan

An extended loan is any period that exceeds more than 48hrs. This will be granted only by the head teacher and a record of the loan will go on the staff record.

- long term equipment loans to be recorded on staff file with the serial number recorded
- any equipment that is on long term loan is returned to school every term for critical antivirus and system updates. This must be arranged with ICT Support
- any damage or failure is reported as soon as the equipment is return
- all laptops will be loaned out with a suitable carry case and necessary charging unit

8.3. equipment must be returned at the end of every school year and/or at the termination of employment with the school.

9. Data breach management

Under the GDPR we must report and log all data breaches with the school Data Protection Lead or Data Protection Officer.

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission; and
- loss of availability of personal data

If you are unsure about whether data has been breached, please discuss with your Data Protection Lead or Data Protection Officer.

It's very important the school know when data has been breached, if the breach is classed as high risk to the data subject we only have 72 hours to report to the Information Commissioner Office.

ICT Acceptable Use Policy (AUP)

Safety and Responsibilities Policy

Staff Acceptance form (academic year 2023/24)

- I understand and agree to abide by the provisions and conditions of this document
- I understand that any violations of the above provisions may result in disciplinary action and revocation of privileges. I also agree to report any misuse of the system to senior staff
- I agree to use the Internet and electronic communication systems in compliance with the terms outlined in this document and in line with data protection regulations and understand that my Internet access any electronic communications may be logged and monitored
- I agree to treat computer equipment with care and respect and understand that any deliberate damage of any form is unacceptable and will result in disciplinary action and / or loss of privileges

I agree to the terms and conditions outlined in his document □ (please tick)

Printed name (capital letters): ……

Role: ……

Signature: ……

Date: ……

Policy update information (policy number GDPR-126)

This policy is reviewed annually and updated in line with data protection legislation.

Policy review information

Review date	Reviewed by
02-01-2020	turn IT on
01-08-2020	turn IT on
02-08-2021	turn IT on
04-08-2021	turn IT on
01-08-2023	turn IT on

Policy update information

Review date	Revision	Description of change	By
02-01-2020	1.00	Draft release	turn IT on
01-08-2020	1.01	Full release	turn IT on