IT Security & Acceptable Use Policy

NON STATUTORY POLICY

Review: Annually

Next Review Date: February 2023

Role	Name
Headteacher	Caroline Rodgers
Chair of Governors	Linda Mosley
Data Protection Officer	Derbyshire County Council GDPR Department
Designated Governor	
Designated Senior Lead	Caroline Rodgers – Headteacher Jayne Saxton – SBO

This document will be reviewed annually and sooner when significant changes are made to the law

Version No: Two

Approval Date: Under Review

Released: February 2021 v3.0

CONTENTS

7.1 Introduction

- The school's IT (Information Technology) infrastructure and digital resources are essential to the effective delivery of education and other activities, but they also present risks to privacy and data protection. We are committed to using IT facilities in a way that meets legal requirements and upholds confidentiality and peoples' privacy rights.
- This policy supports business continuity, data protection and cyber security, and explains how we use technology in line with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018), and other relevant legislation.

7.2 Scope and Responsibilities

This policy applies to:

- The use of school provided IT hardware, software, devices, digital content, networks and communications or those maintained on the school's behalf.
- Personally owned devices which are used for accessing school systems or those which impact on the school or members of the school community.
- All those who access school systems including pupils, staff, visitors, governors, contractors and those working on behalf of the school referred to as "Users" throughout this policy.

All Users are responsible for reading, understanding and complying with this procedure if they have access to IT. Whilst this policy applies to all Users, the school understands that pupils will need additional support to understand how to use IT systems safely and securely.

7.3 IT Acceptable Use Standards

All Users must:

1. Protect school IT resources by careful and considerate use of equipment and networks, reporting faults and minimising the risk of introducing computer viruses or similar to the system.
2. Protect individuals from harmful or inappropriate material accessible via the Internet or transportable on computer media.
3. Protect the confidentiality of individuals and of school matters and safeguard Users by complying with relevant legislation, including:
    - Data Protection Act 2018
    - Privacy and Electronic Communications Regulations
    - Copyright, Designs and Patent Act 1988
    - Computer Misuse Act 1990
    - Counter-Terrorism and Security Act 2015 (encompassing the "Prevent Duty"
    - The Regulation of Investigatory Powers Act (RIPA) 2000
    - WEEE Regulations 2006, the Environmental Protection Act 1990, the Waste Management Regulations 2006.

Users should understand and adhere to their signed Acceptable Use Agreement.

7.4 Roles and Responsibilities

Everyone who works for Brockley Primary School has a responsibility to ensure that data is collected, accessed, stored and handled appropriately and lawfully. Every user must ensure that they adhere to this policy in order to meet the legal obligations of the school and their individual obligations.

The school's Board of Governors, whilst ultimately responsible for ensuring the school meets its legal obligations, is assisted directly by the senior leadership team.

Breaches of this policy should be reported to Headteacher and/or the Data Protection Lead in the first instance.

7.5 Principles of Use

For the purpose of this policy, the use of the internet will include associated internet enabled technologies such as video messaging or conferencing applications.

- Internet and email use is integral to the effective delivery of services provided by the School. Nothing in this policy should be read as restricting the proper use of email, Internet or associated technologies for School purposes.
- Limited personal use of the School's Internet is permitted subject to these principles and guidance notes.
- Personal use of the Internet is only permitted in your own time (e.g. before or after work and during your lunchtime) and limited to browser-based activities.
    - Any personal use must not, in any way, distract staff from the effective performance of their duties. Improper or inappropriate personal use of the School's email, Internet and associated systems may result in disciplinary action.
- Users are not allowed use of the School's email system for personal communication.
- If you feel you may have accidentally breached this policy, you should contact your line manager immediately, or, in their absence, a more senior manager who will record this information. See Unacceptable Use – Section 5.
- The School reserves the right to maintain and review logs of internet, video messaging or conferencing applications, instant messaging (IM) and email use. Auditing and monitoring of school services may form part of disciplinary procedures.
- The School has in place a process to block categories of internet sites and individual sites if it is deemed appropriate. No user should attempt to bypass security measures or processes.
- Any personal information sent via email, the Internet and associated services such as video messaging or conferencing applications, is covered by the Data Protection Act 2018. All staff are required to handle personal information in accordance with the Data Protection Act and the GDPR.
- Emails, including conversations recorded using facilities such as Video messaging or conferencing applications, are covered by the Freedom of Information (FOI) Act and may be disclosed as part of an FOI request for information, or as part of any legal proceedings. Always exercise the same caution on email content as you would in more formal correspondence.
- Whilst school security provides additional protection and real-time scanning security measures cannot guarantee that external communications do not contain malicious content or links. Users should follow security guidance at all times. Consent must be obtained for any recordings of conversations resulting from the use of facilities such as video messaging or conferencing applications.

- The School reserves the right to withdraw Internet access or email use or any access to the School's computer or communications network, if the User has been found to be in breach of this policy.
- Desktop and document sharing capabilities via facilities such as Video messaging or conferencing applications, must only be used with colleagues of the School for collaboration purposes. If you allow changes to be made to these documents during a desktop sharing session as the 'sharer' of the document, it is your responsibility to ensure that the documentation is used correctly and saved appropriately.
- The school requires external suppliers of services to confirm their acceptance of this policy in order to protect the school's network and information assets. Any maintenance and support contracts are agreed and signed in accord with the content and spirit of this Policy

7.6 Email

7.6.1 Personal Use

Personal use of school derbyshire.sch.uk email or any other email system provided exclusively for use as a School employee, is not permitted at any time.

It is inappropriate to use your school address for personal use as it may give the impression that any business is on behalf of the School.

If a genuine emergency arises Users should inform their line manager at the earliest opportunity that they have responded to the email and managers will make a note of it. Users should inform the sender that personal use of the School's email system is not permitted and provide an alternative email address or an alternate method of communication.

7.6.2 Email Usage

Users must only use School provided email systems to send and receive School information.

If Users receive an email that is inappropriate or abusive, they must report it to their line manager immediately, who will take the appropriate action. If the sender is known to the user, they should inform the sender that they should cease sending the material.

Users must not use anonymous mailing services to conceal their identity when mailing through the Internet, or falsify (spoof) emails to make them appear as if they have been sent from someone else.

All employees are required to maintain the good reputation of the School when using Internet and email. Users must not use the email system in any way that is insulting or offensive.

Use of email and the Internet which brings the School into disrepute may result in disciplinary action.

7.6.3 Email Disclaimer

A disclaimer is automatically attached to all emails sent from the School informing the recipient that the email is intended solely for them, is confidential, may be legally privileged and may contain personal views that are not those of the School.

7.6.4 Access to email

Where an employee is absent, the employee's line manager may authorise access to a School email account to obtain messages that are work-related. The manager will inform the employee of this access on the employee's return.

The content of all emails may be viewed by the School in certain circumstances; for example, in connection with disciplinary investigations or audit reviews.

7.6.5 Email Security

Emails containing personal or sensitive information must be sent securely. Any authorised personal data sent externally by email must be sent with encryption enabled or via a password protected file with the password sent via alternative means e.g. telephone.

All senders must ensure the appropriate secure email method is chosen according to the circumstances of the destination of the email.

Senders of any controlled/restricted email must be extremely vigilant about verifying the recipients email address to ensure sensitive data is not sent to the wrong individual/s, leading to a data breach.

Personal data sent to the incorrect recipient should be reported in line with school's data breach procedure.

When emailing multiple recipients, the 'TO' box should be addressed to an address within the organisation (eg info@school-derbyshire.sch.uk) and the BCC option (blind copy) chosen to add multiple email addresses so addresses are not disclosed.

Email security is required to meet with the requirements of The Data Protection Act 2018

7.6.6 Email Retention

Emails should only be kept in your inbox for a recommended time of 3– 6 months, which is reflected in the retention schedule. Any emails that you need to keep beyond this period should be saved to appropriate file storage. For further information, please refer to the school's retention schedule.

All electronic communications, whilst they are held by the school, are disclosable under data protection legislation and anything written or held, within an email, could potentially be released under the terms of a Subject Access Request.

7.7 Instant Messaging (IM)

Instant Messaging is a form of real time communication between two or more people based on typed text. The text is conveyed via devices connected over the Internet or an internal network/intranet. Messages are retained in your conversation history in your email folder list or are saved as emails in your inbox if the recipient does not respond immediately.

You must only use School provided internet messaging (IM) services. IM should not be used as a substitute for email. IM should be used only for questions or announcements that are short and need to be communicated immediately.

Private use of instant messaging for any purpose is not permitted.

More information on the use of other social media can be found in the School's Social Media Policy.

7.8 Internet Use

7.8.1 Personal Use

Personal use of the Internet is not allowed during working hours. You can use the Internet before you start work, during your lunchtime, or after work. You must not, in any way, distract others from their work.

You must not use the School's Internet or email systems for trading or personal business purposes.

You are advised not to conduct online payments. This is due to the information being stored locally on your computer, which potentially could be compromised, putting the user at financial risk. If you use the Internet to buy goods or services, the School will not accept liability for default of payment or for security of any personal information you provide. Goods must not be delivered to a School address.

All Internet sessions should be terminated as soon as they are concluded.

7.8.2 Filtering Content

Many Internet sites that contain unacceptable content are blocked automatically by the School's systems. However, it is not possible to block all "unacceptable" sites electronically in all circumstances.

Attempting to bypass or disabling filtering, proxy or security settings is strictly forbidden without written authorisation.

Where it is necessary to disable services temporarily, the business need for the action will be documented and the risks assessed. Approval from the headteacher must be sought and services must be re-enabled / any open ports closed, as soon as possible.

Filtering requirements form part of the Prevent Duty, as enacted in the Counter-Terrorism and Security Act 2015.

7.8.3 Downloading Material

Downloading of video, music files, games, software files and other computer programs is not permitted. These types of files consume large quantities of storage space on the system (and can slow it down considerably) and may violate copyright laws.

Streaming media, such as radio or TV programmes, for non-work related purposes is not permitted.

If you are in doubt about software use or installation, seek guidance from the Data Protection Officer.

7.8.4 Accidental Access to Inappropriate Material

You may receive an email or mistakenly visit an Internet site that contains unacceptable material. If this occurs, you must inform the Headteacher or a member of the Senior Leadership Team immediately.

The Headteacher or Senior Leadership Team Member will ask you for details relating to the incident and you will be asked how the event occurred. This information may be required later for management and audit purposes.

7.8.5 Copyright

Most sites contain a copyright notice detailing how material may be used.

If you are in any doubt about downloading and using material for official purposes, you should seek legal advice and ensure compliance with the Copyright, Designs and Patents Act 1988

You may be in violation of copyright laws if you simply cut and paste material from one source to another. All sources used for research purposes should be referenced appropriately and credited.

7.8.6 Unacceptable Use

You must not deliberately view, copy, create, download, save, print or distribute any material that:

- is sexually explicit or obscene
- is racist, sexist, homophobic, harassing or in any other way discriminatory or offensive
- contains material the possession of which would constitute a criminal offence
- promotes any form of criminal activity
- contains unwelcome propositions
- involves gambling, multi-player games or soliciting for personal gain or profit
- contains images, cartoons or jokes that may cause offence
- appears to be a chain letter
- brings the School into disrepute or exposes it to legal action

This list is not exhaustive and the School may define other areas of unacceptable use.

Unacceptable use may be reported to the police if likely to constitute a breach of the Computer Misuse Act 1990.

7.9 Monitoring

The School is able to produce monitoring information, which may include email usage statistics, frequent email contacts, file sizes and may lead to further enquiries being undertaken.

The School is also able to record the details of all Internet traffic to protect the School and its employees from security breaches, including hacking, and to ensure that "unacceptable" sites are not being visited.

Any potential infringement will be referred to Senior Leaders as part of routine reviews.

The School may read and inspect individual emails and attachments for specific business purposes or during disciplinary investigations including:

- Establishing the content of transactions,
- Ensuring employees are complying both with the law and with the School's email policy, and
- Checking emails when employees are on leave, absent or for other supervisory purposes.

The School's email system records details of all emails sent and received. The system filters the use of certain prohibited words and may limit file sizes.

Monitoring logs may include:

- The network identifier (username) of the user
- The address of the Internet site being accessed
- Where access was attempted and blocked by the system
- The web page visited and its content
- The name of any file accessed and/or downloaded

- The identity of the computer on the network and the date and time

Any excessive or inappropriate use may result in disciplinary action being taken.

Monitoring is encompassed in The Regulation of Investigatory Powers Act (RIPA) 2000

7.10 Passwords

Access to applications and information is controlled to protect Users and the school.

It is important that the passwords are strong and safe enough to keep data secure. The minimum length of passwords required for school systems is 8 characters, although 12 characters are recommended.

Strong passwords include upper and lower case letters, numbers and special characters like asterisks or currency symbols.

Passwords should not be written down or shared. Passwords must be difficult for others to guess.

The school recommends the use of a Password Manager to aid Users in keeping track of passwords. A number of these are available without charge.

Where two factor authentication (2FA) is provided, such as a pin, passcode or additional verification data, this should be used.

Personal devices used for accessing school systems must be secured by a device lock which requires a password, pin or biometric method to unlock. Please refer to the BYOD policy for more information.

When choosing your passwords, don't choose a password based on any personal data such as your name, age, or your address. Avoid using anything which can be easily guessed or identified.

Advice on choosing a secure password is available from the NCSC.

7.10.1 Methods for choosing passwords

1. Initial letters from each word in a sentence:

   My uncle Joe walks his 3 dogs in the park every morning - MuJwh3ditpem

   I like to eat Ben & Jerry's ice cream for dinner - IlteB&Jic4d

2. Three random words

   brown house bears - BrownHousebearS (or Br0wnH0usebear$)

   jump yelling sat – JumpYellingSAT (or JumpY3llingS@T)

You can add extra punctuation, special characters and numbers to your password and turn numbers into digits for added security.

7.11 Loaned IT Equipment

Devices issued to staff remain the property of the School and is provided to Users on a loaned basis. The device must not be used by anyone other than the authorised user to whom it has been allocated.

Any device property identification should not be altered or removed for any reason.

Users who borrow equipment from the school must sign for it and bear the responsibility for its care.

All reasonable care should be taken to prevent loss, damage, theft or unauthorised use of IT equipment as far as is practical. For example, devices should never be left in a vehicle overnight or other unsecured, vulnerable situation. See the Offsite Working Procedure for more guidance.

Any loss or damage to equipment on loan should be immediately reported to the Headteacher of Senior Leadership Team Member in the first instance and any theft or criminal damage should be reported to the Police.

Where there is evidence that the equipment has not been used in accordance with policy, a charge may be made for the replacement or repair of any school equipment whilst on loan.

7.12 Bring Your Own Device (BYOD)

To prevent data loss and ensure consistent application of School policies, no personally owned equipment should be attached to the School's network without the permission of the Headteacher.

Please refer to separate the Bring Your Own Device (BYOD) Policy

7.13 Software, Updates and Patching

School devices have a predetermined list of software installed on the hard drive.

Users should use software in accordance with applicable licence agreements. It is a criminal offence to copy software or any supporting documentation protected by copyright.

The use, or possession of unlicensed copies or "pirated" versions of software is illegal and is expressly prohibited by the school.

No addition or deletion of any software or hardware (except peripherals) is permitted without the express permission of the Head Teacher or designated IT lead. This includes the setting up of web-based accounts.

Software and web-based accounts that require personal data may be subject to a Data Protection Impact Assessment and so must not be installed or set up until this has been carried out.

To ensure that security patches and virus definitions are up to date staff should connect devices to the School network on a regular basis. Updates must be allowed to run and should not be interrupted.

Staff should make careful, considerate use of the school's IT resources, report faults and work in a way that minimises the risk of introducing computer viruses into the system.

7.14 Network Access and Data Security

7.14.1 Users Authorisation

Those accessing information systems, data or services will be authorised to do so by an appropriate authority, usually the line manager.

Changes to access must be requested and authorised. Users who believe they have access to systems they no longer need, must report this to their line manager.

Users must only access information held on the School's computer systems if authorised to do so and the information is needed to carry out their work.

Line managers will only request the minimum access required for the user to carry out their work.

A record of user access to systems will be maintained and periodically reviewed.

7.14.2 Starters and Leavers

Line managers must ensure that access to IT Systems is only available to employees during their period of employment and withdrawn as soon as employment is terminated.

A new starter's form will be completed by line managers as part of the induction process, detailing:

1. The names of the systems new starters have been given access to
2. The date the access was enabled
3. The level of access (role)
4. The name of the authoriser

At the end of employment this form will be used to ensure access to each system has been removed and by whom.

When a contract of employment at the School ends, the member of staff must return all equipment, including peripherals, to the School in full working condition.

It is the responsibility of the user to backup any data or documents they may require, prior to returning the device. Any data pertaining directly to the school or members of the school community **must not** be retained.

The user account and all personal work stored on the laptop will be securely deleted upon return.

7.14.3 External Support Access

Staff providing temporary guest logins for external support services providers must ensure that system access does not extend beyond the requirements of the activities needed to support the provision of services.

Those requesting/providing temporary access must also ensure that system access is withdrawn as soon as the affiliate's relationship with the school ceases.

7.14.2 Confidentiality

Under no circumstances should personal or other confidential information held on the school network or IT equipment be disclosed to unauthorised persons. If you accidentally access information which you are not entitled to view report this immediately to the Head Teacher or Data Lead as a data breach.

Staff must ensure that confidential or sensitive data is not accessible unauthorised persons by logging off or locking the computer when it is left unattended.

In classrooms, screens must be set to **extend** to the Interactive whiteboard rather than **duplicate** and when using screen sharing facilities, Users should fully minimise screens with any sensitive data / emails.

7.14.3 Security of Portable Devices

The school allows the use of encrypted USBs.

Sensitive or confidential information should be accessed via the network and should not be permanently stored on portable devices e.g. memory sticks / laptops / tablets.

Where the use of a memory stick to transfer or store data temporarily is unavoidable, this must be done using an encrypted memory stick provided by the school.

All school devices used to store personal information will be fully encrypted.

7.14.4 Physical Security

Building access and physical controls protect areas where sensitive or confidential information is processed. Server access and access to network equipment, telecoms and network access points is restricted to those staff with authorisation.

7.14.5 Administrative Access

- Administrative accounts and credentials must use strong authentication / complex passwords.
- Administrative accounts must not be used for general activities, especially those of high-risk, such as browsing the internet or emailing.
- Administrative access is only provided to designated staff and a review of administrators for each system will be carried out annually, in line with the software audit.

7.15 Disposal of Computing Resources

Computing resources will be disposed of in line with WEEE regulations, The Hazardous Waste Act, The Environmental Protection Act 1990, The Environment Act 1995 and The Data Protection Act 2018

1. Governor approval will be sought before Computing resources are disposed.
2. Following Governor approval, all equipment which contains sensitive files will have their hard disk drives wiped and all sensitive or confidential data and licensed software will be irretrievably deleted during the disposal process.
3. Damaged devices containing sensitive or confidential data will undergo assessment to determine if the device should be destroyed, repaired or discarded.
4. If a third party contractor is used, suppliers will be suitably accredited and disposal certification will be obtained.
5. Finally, the school's inventory will be updated.

7.16 Backup Procedures

If software/hardware problems arise, a device may need to be restored to its original settings. Work files may be lost during the restore process, therefore it is the responsibility of all Users to ensure that files are saved to network drives.

Removable storage, such as encrypted USB's are not backed up by the routine backup process and Users take responsibility for carrying out a manual backup process.

The School ensures that systematic backup of data is completed on a regular basis so that recovery of essential data can be managed in the event of loss of data files or system failure.

School Process	**On-site / off-site**	**Frequency** (daily/weekly/monthly)
Main File Server	On-site server and back-up	100g back-up is completed daily to the cloud

School MIS	Cloud Based Storage Data is stored in a secure UK datacentre.	Weekly Backup A full backup of all of your data is taken every Friday evening. This is to ensure RM have a complete copy of your data on a weekly basis Daily Backups Every evening RM take a Differential backup of your data. This means RM compare the data shown in your schools database with the backup we took the previous evening and we backup any data which has changed. This means we have an easy to access backup if you report an issue with data within 24-48hrs of the issue.
Email Server	Offsite – Office 365	Microsoft also keeps a 14-day backup of Office 365 data and a backup is created every 12-hours. Microsoft 365 Cloud Backup is a **cloud-to-cloud backup** solution that automatically and securely backs up Emails/Attachments, calendars, contacts, tasks, OneDrive, SharePoint, Groups and Teams and includes powerful search and recovery tools.
Curriculum Files	On-site server and back-up	100g back-up of data is completed daily to the cloud
Administration Files	On-site server and back-up	100g back up of data is completed daily to the cloud
Website	Offsite	Daily

Backup copies will be securely stored against theft, corruption or physical damage, so that in the event of a major incident a backup copy is available.

The backup is cloud based and protected in the event of an incident. Rotation of data for administration, curriculum file and the man file server does not take place.

7.17 Disaster Recovery Procedures

In the case of a disaster staff should refer to the IT Disaster Recovery Plan / Critical Incident Plan and ensure the following are readily available:

- An up to date list of contacts to assist in the recovery process, e.g. head teacher /IT provider.
- A list of procedures and actions required by key individuals in the event of a critical incident.

Any contingency plan must take into account any possible staff changes, be easily accessed and should be read and understood by all relevant stakeholders.

The school should ensure all items are appropriately insured.

7.18 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to School assets, or an event which is in breach of the School's security procedures and policies.

All School employees, supply staff, governors, contractors, and volunteers have a responsibility to report security incidents and breaches of this policy as quickly as possible through the School's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the School

The School will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place.

Suspected misuse of the School's computer systems by a member of staff will be considered by the Headteacher and Governors. In the case of an individual then the matter may be dealt with under the disciplinary process.

Review Date	Details of Changes	Name	Approval Date	New Version No	Website
29.1.22	New policy cover sheet and amendment page added Page Numbers updated Section 7.4 – School name inserted in first paragraph Section 7.4 wording added to last sentence 'Headteacher and/or the Data Protection Lead' Section 7.6.6 – wording inserted 'inbox for a recommended time of 3– 6 months, which is reflected in the retention schedule.' Section 7.8.4 wording inserted 'Headteacher or a member of the Senior Leadership Team' Section 7.11 wording added 'Headteacher of Senior Leadership Team Member' Section 7.14.2 wording inserted 'Head Teacher or Data Lead' Section 7.14.3 wording inserted 'allows the use of encrypted' Section 7.16 – Back up Procedures table completed with the organisation information	ES JS JS JS JS JS JS JS JS JS		Two	Yes