IT Security and Acceptable Use Policy

Kirk Langley C.E. Primary School

Last Reviewed	Summer 2024
Reviewed By (Name)	B Wood
Job Role	Business Manager
Next Review Date	Summer 2025
Next Review Date	Summer 2026
Next Review Date	Summer 2027
Version released Spring 2024	

Kirk Langley Church is a England of School Primary family and our that believe Child ‘Every Shine.’ Can visions Our values, and the living built on Gospel of Christ within daily life, are at the core of everything we do. They underpin our teaching and learning and provide an environment which prepares our pupils in being respectful, confident, thriving citizens.

Daniel 12:3

'Those who have insight will shine brightly like the brightness of the expanse of heaven, and those who lead the many to righteousness, like the stars forever and ever.'

Copyright: Education Data Hub

We aim to provide a thriving, inspiring and stimulating learning environment where children achieve the very best they are capable of because all the staff value their different learning styles. Kirk Langley Church of England Primary School is committed to Christian values where children, parents/carers and our community know us by our actions.

Within a Christian ethos we aim to:

- Promote a positive attitude to life-long learning, nurturing the development of self-esteem; leading to aspirational, independent learners that are prepared to be challenged and take risks in a diverse and ever changing world.
- Provide the children with valuable experiences and opportunities, through a broad, balanced and exciting curriculum, where learning is purposeful and engaging.
- Use a variety of teaching strategies and resources effectively and creatively; encouraging each child to progress and attain to the highest possible standards, in relation to their age and ability.
- Strongly believe in the partnership of parental involvement in the education of our pupils.
- Demonstrate and foster respect for ourselves and others within the school, local community and the global community.
- Respect the belief of others and celebrate cultural diversity.
- Encourage spiritual and moral values.
- Explicitly promote the fundamental British values of democracy, the rule of law, individual liberty and mutual respect and tolerance of those with different faiths and beliefs through a 'living' curriculum.

Value each child as an individual within the school and respect personal beli

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

Guidance from the Department for Education about school policies can be found here: https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts/statutory-policies-for-schools-and-academy-trusts

CONTENTS

1. Introduction.....5

Copyright: Education Data Hub

2. Scope and Responsibilities 5
3. IT Acceptable Use Standards 6
4. Roles and Responsibilities 6
5. Principles of Use 7
6. Email 8
6.1 Personal Use 8
6.2 Email Usage 8
6.3 Email Disclaimer 8
6.4 Access to email 9
6.5 Email Security 9
6.6 Email Retention 9
6.7 Out of Office 10
7. Instant Messaging (IM) including Microsoft Teams 10
8. Recording calls / meetings / online lessons / staff training 10
8.1 Recording telephone calls 10
8.2 Recording meetings 11
8.3 Recording online lessons 11
8.4 Recording staff training 11
9. Internet Use 11
9.1 Personal Use 11
9.2 Filtering Content 11
9.3 Downloading Material 12
9.4 Accidental Access to Inappropriate Material 12
9.5 Copyright 12
9.6 Unacceptable Use 12
10. Monitoring 13
11. Passwords 14
12. Loaned IT Equipment 14
13. Bring Your Own Device (BYOD) 14

Copyright: Education Data Hub

14. Software, Updates and Patching.....14
1.5 Network Access and Data Security.....15
15.1 Users' Authorisation ..... **Error! Bookmark not defined.**
15.2 Confidentiality..... **Error! Bookmark not defined.**
15.3 Security of Portable Devices ..... **Error! Bookmark not defined.**
15.4 Physical Security..... **Error! Bookmark not defined.**
15.5 Administrative Access ..... **Error! Bookmark not defined.**
16. Backup Procedures.....16
17. Disaster Recovery Procedures.....16
18. Breaches of Policy 17

Copyright: Education Data Hub

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 data protection, online safety and safeguarding. 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 (UK GDPR) and the Data Protection Act 2018 (DPA 2018), the Departments for Educational Digital and Technology standards in schools and colleges and other relevant legislation.
- In line with the Department for Education's *Digital Accessibility* standards, the school has due regard to ensuring that digital systems, content, and services are accessible and usable for all members of the school community regardless of individual needs or circumstances.
- This policy should be read in conjunction with the school HR advice and guidance. This policy does not stand alone, it is essential to follow the requirements set out in the Derbyshire LA Acceptable Use of IT Advice and Guidance, which provides more details as well as guidance to Governing Boards.]

  This policy has been the subject of formal negotiation and consultation between Derbyshire County Council and the recognised Trade Unions and Professional Associations. Agreement and adoption were only reached by Schools Joint consultative Committee where it is used in conjunction with the DCC LA Acceptable Use of IT Advice and Guidance.

2. Scope and Responsibilities

This policy applies to:

- The use of school-provided (or provided for the school's use) IT hardware, software, devices, digital content, networks and communications.
- Non-school owned devices which are used for accessing school Internet or information systems or used in a way which impacts on the school or school community.
- All those who access school systems including pupils, staff, visitors, governors. These are all referred to as "Users" throughout this policy. Staff must have due regard to digital accessibility when creating or using digital content and systems.
- Users must immediately report any actual or suspected misuse of digital systems, loss of data, unauthorised access, or safeguarding concern arising from digital activity in line with the school/trust/academy's Incident Reporting and Safeguarding procedures.
- 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.

Copyright: Education Data Hub

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 electronic media.
3. Only use Artificial Intelligence applications in line with the school's Artificial Intelligence Policy, Guidance Document and the Privacy Notices.
4. Protect the confidentiality of individuals and of school matters and safeguard Users by complying with relevant legislation, including:
    - Data Protection Act 2018 and General Data Protection Regulation
    - 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
    - Waste Electrical and Electronic Equipment Regulations 2006, the Environmental Protection Act 1990, the Waste Management Regulations 2006.
    - The Department for Education Digital and Technology Standards for Schools and Colleges
5. Keeping Children Safe in Education 2025(KCSIE)
6. Users should understand and adhere to their signed Acceptable Use Agreement.

In practice, this requires Users to apply the principles of data minimisation, purpose limitation and confidentiality when using digital systems. Users must not access, create, share or retain personal data unless it is directly required for their role.

4. Roles and Responsibilities

Everyone who works for Kirk Langley C.E. 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 the headteacher in the first instance.

Copyright: Education Data Hub

5. Principles of Use

For the purposes of this policy, use of the internet includes all school/trust/academy-provided or approved internet enabled technologies and digital services. This includes, but is not limited to, cloud-based systems (such as Microsoft 365, management information systems, safeguarding and remote-learning platforms), email, video and audio calls, instant messaging, webinars, and online meeting 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 permitted to use of the School's email system for personal communication.
- The School reserves the right to maintain and review monitoring and activity logs of the school Digital services including the internet and associated internet-enabled technologies including emails, video calls, video messaging, instant messaging, webinar applications or conferencing applications and email use. Auditing and monitoring of the use of school IT 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. Users must not attempt to bypass security measures or processes.
- Any personal information sent via email, the Internet and associated internet-enabled services is covered by Data Protection legislation. All staff are required to handle personal information in accordance with the Data Protection Act 2018 and the UK GDPR.
- Emails, including conversations recorded using facilities such as video calls, instant 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, video calls, instant messaging or conferencing applications as you would in more formal correspondence.
- Whilst school security provides additional protection and real-time scanning, our security measures cannot guarantee that external communications do not contain malicious content or links. All staff with access to the IT network must take basic cyber security training annually in line with DfE Cyber Security Standards. and RPA insurance term and conditions
- Consent from all parties must be obtained before recording conversations when using facilities such as video calls, instant messaging or conferencing applications.

Copyright: Education Data Hub

- 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 is found to be in breach of this policy.
- Desktop and document sharing capabilities via facilities such as video calls 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.

6. Email

6.1 Personal Use

Personal use of school email is not permitted. However, communication with a Trade Union is not considered personal use.

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.

6.2 Email Usage

Users are not permitted to send and receive School related information from personal email accounts. Users must only use School provided email systems. However, staff are permitted to forward emails to their Trade Union representative via their personal email account, for the purposes of seeking advice.

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 to cease sending the material.

Users must not use anonymous mailing services to conceal their identity 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 unprofessional inappropriate or harmful.

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

6.3 Email Disclaimer

A disclaimer is automatically attached to all emails sent from the School system 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.

Copyright: Education Data Hub

6.4 Access to email

When a member of staff is absent, their line manager can authorise access to a School email account solely for the purpose of retrieving work-related messages that are work-related. The manager will inform the member of staff of this access on their 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.

6.5 Email Security

Users will be vigilant of phishing emails or other scams when using the school's email system by being mindful of cyber security considerations, particularly when opening and responding to emails, or being prompted for a login in directly from an email. Annual cyber security training will inform of the latest trends in email security. Users will follow the schools/trust reporting procedures should they receive a suspect email.

Emails containing sensitive personal data, or otherwise sensitive information, must be sent securely. Any 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 recipient's 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.sch.uk) and the BCC option (blind copy) chosen to add multiple email addresses so addresses are not disclosed.

6.6 Lawful Email Monitoring

Monitoring and access to email communications are not based on individual consent, but are carried out where necessary for operational, safeguarding, legal or security purposes. Further details are outlined in our monitoring section.

6.7 Email Retention

Emails will automatically be deleted after 13 months. 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 potentially disclosable under data protection legislation and anything within an email could be released in response to a Subject Access Request.

Copyright: Education Data Hub

6.8 Out of Office

Email accounts should return an Out of Office message during school holidays. This will indicate whether or not emails will be monitored and when the school reopens. Similarly, during periods of extended staff absence an Out of Office message should refer senders to an alternative or general school email address.

7. Instant Messaging (IM) including Microsoft Teams

Instant messaging (IM) systems provide real-time text-based communication between users.

- Staff must only use school/trust/academy-provided [school to delete as appropriate] or approved instant messaging platforms. Personal or private use of instant messaging on school systems is not permitted.
- IM should be used within approved professional contexts, for work-related communications. Instant messaging must not be used as a substitute for email or other formal communication channels where a permanent and structured record is required.
- In line with KCSiE, staff must maintain professional boundaries when using instant messaging tools. This includes:
    - avoiding one-to-one private messaging with pupils where this is not authorised or appropriate.
    - ensuring communications with pupils are transparent, appropriate, and, where possible, take place in group or moderated channels.

All use of instant messaging is subject to monitoring and record retention in line with this policy and relevant data protection and safeguarding requirements. Staff must report any concerns arising from instant messaging use, including inappropriate content, conduct, or safeguarding concerns, to the Designated Safeguarding Lead (DSL) in accordance with safeguarding procedures.

Commented [PW1]: It is my understanding that all interactions should be monitored no “where possible”

Further guidance on online communication and social media use is set out in the school’s/trust’s/academy’s Social Media Policy.

8. Recording calls / meetings / online lessons / staff training

Recording calls, meetings, online lessons, etc will generate personal data including pupil images, names, contributions, and contact details and will be protected, processed and retained in the same way as all personal data, in line with the school’s Data Protection Policies and Privacy Notices and in accordance with our other policies including Off Site Working and Bring Your Own Device policies, as well as our Retention Schedule. The school recognises that recording staff whilst at work may be considered to be privacy intrusive and therefore careful safeguards will be put in place should recording be deemed necessary. In particular, the school must ensure that the Data Protection principles as set out in the Data Protection Policy (“Our DP rules”) are adhered to. Only authorised tools and software will be used for these purposes (see our AI policy).

We will never record calls, meetings, online lessons or staff training in a covert manner.
Recordings in these circumstances will be carried out in line with our HR policies and procedures.

8.1 Recording telephone calls

We do not record incoming and outgoing telephone calls.

Copyright: Education Data Hub

8.2 Recording meetings

We may record meetings. The purpose of this is to ensure minutes and notes taken are an accurate record. Attendees will be informed if the meeting is to be recorded. Recordings will be securely destroyed as soon as the minutes have been approved. Recordings will be available to attendees until minutes are approved and the recording destroyed.

8.3 Recording online lessons

We do not record online lessons

8.4 Recording staff training

We may record staff training. The purpose of this is to ensure the training is available to staff who were unable to attend live. Attendees will be informed if the training is to be recorded. Protocols regarding cameras, chats and contacts will be outlined at the start of each session. Additional information about our lawful basis, processors, use and retention period can be found in our Privacy Notices and Retention Schedule.

9. Internet Use

9.1 Personal Use

Personal use of the Internet is not allowed during working hours. You can use the Internet, for browser-based activities only, 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 browsing sessions should be terminated as soon as they are concluded.

9.2 Filtering Content

The school has filtering systems in place to block harmful and inappropriate online content, in line with statutory safeguarding requirements. While filtering systems reduce risk, they cannot guarantee that all inappropriate content will be blocked.

Any access to inappropriate content, whether accidental or otherwise, must be reported immediately to the DSL for assessment and action.

Users must not attempt to bypass, disable, or undermine filtering, monitoring, proxy, or security controls under any circumstances.

Where changes to filtering or monitoring settings are required for legitimate educational or operational reasons, the User must request the change through Headteacher] so that the rationale can be documented in accordance with the DfE Filtering and Monitoring Standards referenced in KCSiE. Such changes must be approved in advance by the

Copyright: Education Data Hub

Headteacher and/or the DSL [delete where appropriate]. Where temporary, the change must be time limited, regularly reviewed, and promptly reverted when no longer required.

Filtering and monitoring arrangements form a core part of the school's safeguarding responsibilities under KCSiE, the Prevent Duty (as set out in the Counter-Terrorism and Security Act 2015), and the DfE Digital and Technology Standards for Schools and Colleges.

9.3 Downloading Material

Users must not download video, music files, games, software files and other computer programs. 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, your IT support and where the system uses personal data your Data Protection Officer.

seek guidance from the Data Protection Officer.

9.4 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 immediately.

The manager will ask you for details of the incident including how the event occurred. This information may be required later for management and audit purposes.

9.5 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 to 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.

9.6 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

Copyright: Education Data Hub

- 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.

10. Monitoring

The school uses technical monitoring systems that track all user and network activity across its devices and services. This includes monitoring on the school network, within Google or MS 365 environments (including Teams or chat), email, internet usage, and telephone/VoIP calls.

Monitoring is conducted for cybersecurity, business continuity, and legal compliance per KCSiE, DfE filtering and monitoring requirements, and relevant cybersecurity standards. Only authorised staff can access monitoring data, which is kept according to the organisation's retention policy and not used for routine performance evaluations.

These monitoring systems alert the correct personnel within the school to any unusual or potentially inappropriate actions—like safeguarding issues or cybersecurity incidents. Any concerning activity is investigated, documented, and, if needed, referred to the Headteacher, Digital Lead, or IT support as part of safeguarding or security processes.

The monitoring systems can generate reports as needed to protect systems, students, and staff from breaches such as hacking and to ensure online content is suitable and complies with KCSIE and DfE Filtering and Monitoring Standards.

The school may read and inspect individual emails and attachments when necessary for legitimate business reasons, including:

- Confirming business communications or transactions,
- Ensuring legal and policy compliance,
- Supporting disciplinary or grievance investigations,
- Accessing vital information during staff absence, leave, or supervisory/safeguarding situations.

Metadata about sent and received emails—such as sender/recipient info, date/time, file size, and attachment type—is recorded. The system can also filter emails by blocking prohibited words or limiting file sizes, supporting safeguarding, security, and data protection.

Misuse of the email system—if excessive, inappropriate, or unauthorised—may result in disciplinary action under the relevant procedures.

All communication monitoring or interception is done lawfully, proportionately, and transparently, in line with UK GDPR, Data Protection Act 2018, and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Only authorised personnel have access to email contents, and only for justified reasons—not as a matter of routine.

Any breach of this IT Acceptable Use Policy detected through monitoring will be reported to the Headteacher/DSL following the school/trust/academy's disciplinary and safeguarding process.

Copyright: Education Data Hub

11. Passwords

Access to digital systems is protected to safeguard users, data, and systems. The school/trust/academy's authentication and password policies are detailed in the Cyber Security Policy, and updates will be provided through official channels.

- Users receive individual accounts with the least privilege needed for their role. Passwords should follow best practices: they must comply with policy, be strong, not written down or shared, avoid personal information, and be changed if compromised. Accounts and credentials must never be used by others.
- An approved password manager is recommended for secure password management. Multi-factor authentication (MFA) is required for high-risk data and admin account access.

12. 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 must 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. Devices should never be left in a vehicle 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 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.

13. 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 Head Teacher.

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

14. Software, Updates and Patching

School devices have a predetermined list of software installed on the hard drive. where a need for additional software is identified it must be requested through the school's process to ensure that the appropriate installation process has been followed.

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

Copyright: Education Data Hub

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 use 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 must connect devices to the School network on a regular basis. Updates must be allowed to run and should not be interrupted. If an update has failed for any reason the User should notify the Headteacher/IT support immediately.

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.

1.5 Network Access and Data Security

15.1 Users' Authorisation

Access to information systems, data and services must be authorised by the headteacher as part of the school's starter, mover and leaver process.

- Users who require changes to access must request this through the agreed authorisation route [enter how e.g. Line manager/SBO/Headteacher/IT support the starter] in accordance with the starter, mover, and leaver process. This includes users who believe they have access to systems or data they no longer require.
- Users must only access information held on the systems where they are authorised to do so and access is necessary to carry out their role.
- Users should report immediately to the appropriate authority (Headteacher) if they believe they have been allocated an incorrect or excessive level of access. Such incidents may require assessment and action in line with the data breach reporting process.

Line managers must only request the minimum level of access required for a user to perform their duties, applying the principle of least privilege.

A record of user access to systems must be maintained and should be reviewed periodically to ensure access remains appropriate.

15.2 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 as a data breach.

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

Copyright: Education Data Hub

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

15.3 Security of Portable Devices

The school does not allow the use of USBs / removable storage devices.

- Staff will access sensitive or confidential information via the network and will not permanently store sensitive or confidential information on portable devices e.g. memory sticks / laptops / tablets /phones. Where the use of a memory stick to transfer or store data temporarily is unavoidable, this will be done using an encrypted memory stick provided by the school. All school devices used to store personal information will be fully encrypted.

15.4 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.

- Staff will not attempt to access restricted points, or allow others to use their [passes, codes or keys] to gain access.
- Staff will report the loss of [passes, codes or keys] immediately following the school reporting process in line with Safeguarding requirements.
- Staff must ensure that portable devices e.g. memory sticks / laptops / tablets /phones are stored securely when not in use to prevent loss, theft, or unauthorised access.

15.5 Administrative Access

- Users with Administrative accounts and credentials will use strong authentication / complex passwords. Current guidance on the authentication and security measures that should be put into place for network devices, filtering and monitoring services and administrative accounts can be found in the DfE Digital Standards.
- Users will not use Administrative accounts for general activities, especially those of high-risk, such as browsing the internet or emailing.

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 or cloud-based networks.

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

17. Disaster Recovery Procedures

In the case of a cyber incident or digital outage staff will follow the guidance given to them by the Disaster Incident Response Team. This is in line with the Cyber Security Policy and the IT Disaster Recovery Plan/Cyber Response Plan.

Copyright: Education Data Hub

For guidance on Kirk Langley Primary School's approach to disaster recovery please refer to the Cyber Security Policy and the IT Disaster Recovery Plan/Cyber Response Plan

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./Governors In the case of an individual then the matter may be dealt with under the disciplinary process.

Copyright: Education Data Hub