Staff responsible	Andy Taylor
Date of policy/last review	17/05/2021
Governing body ratified	22/05/2018
Chair of Governors	
Review cycle	3 years
Next review	17/05/2024

1. Purpose and Audience

1.1 This policy covers the handling and security of Brent Knoll School's information, in electronic or other media. (It may sometimes make reference to paper)

1.2 This policy's objective is:

- To ensure confidentiality, availability and accessibility of the schools information at all times.
- To ensure schools information, computers and systems are protected against internal threats.
- To minimise the damage and risk that could result from unauthorised access to information.
- To ensure that all ICT users are aware of their obligations and the risks of not complying with this and other policies.

2. Principles of Security

2.1 The school's information is valuable information that must be protected to ensure business continuity, to avoid breaches and meet statutory, regulatory and contractual obligations.

2.2 Much of the information collected by Brent Knoll School includes data about school staff, children and their families which could include vulnerable adults and children. It is the School's duty to ensure that its data is not put at risk because of poor information security.

3. Roles and responsibilities

3.1 Headteacher

- Responsible for ensuring the application of effective information security measures
- Responsible for creating security policies, procedures and guidelines
- Responsible for signing off security policies
- Responsible for promoting security awareness and ensuring staff understand its importance

3.2 All staff

- Responsible for maintaining effective security in the way they work and to ensure that the School's information is protected as set out in this policy.

4. Personal Interest

4.1 The school will hold some information about members of staff. Lewisham's HR department will have staff personnel files and there may also be information about other people that you know or who are members of your family on your school premises.

4.2 You are not allowed to access any of this information for your own purpose or because someone else has asked you. This amounts to unauthorised access to information. If you require information about yourself you should contact your line manager or HR.

5. Accessing and retaining information

5.1 You will need to access information in order to do your job, but should not have access to personal, sensitive or confidential information if it does not relate to your job role.

5.2 You should only have access to school's physical data and any systems you need in order to do your job.

5.3 You must not keep information longer than is necessary. The school is required to maintain all information, regardless of what format it exists in for a set period of time. This is known as the files retention period.

5.4 This means you must use proper housekeeping of cupboards, files, folders, computers, systems and mailboxes.

5.5 You must use approved secure disposal methods for paper records and IT kit disposal.

5.6 You must:

- Only access information or systems that you are entitled and authorised to use
- Protect the school's information at all times – whether in paper or electronic form
- Only use information for the purposes for which the school has collected it
- Delete or dispose of information securely when it is no longer needed in line with the school's retention schedule

5.7 It is an offence, under the Freedom of Information Act 2000 to delete any information subject to an FOI request once a request has been made. This includes e-mail.

6. Sharing Information

6.1 Information sharing is essential for the school to work effectively. Much of the schools work is governed by legislation and therefore this information must be shared for the vital and legitimate interests of the children.

6.2 Any information the schools needs to share externally (and is not governed by legislation), either for a one off, regular or permanent basis then you may need to have an Information Sharing Agreement in place if there is no contract or the contract does not adequately cover data protection or other relevant legislation.

6.3 If you believe this type if sharing is happening and it is not being recorded, let your line manager know.

6.4 It is important unless detail is key, to minimise the data you share as much as possible. Only share what you absolutely must.

6.5 Electronic documents can be redacted using procured software. (If applicable)

6.6 If a black marker is used for paper documents, ensure that the redacted information cannot be viewed. If data is still viewable a photocopy of the redacted information should be provided and not the original.

7. Sharing Information

7.1 It is important to keep your working environment clean and tidy in order to practice good records management. For more information on this refer to the Records Management Policy.

8. Password Management

8.1 Effective username and password combinations must be used to avoid unauthorised access to school systems.
8.2 Make passwords as complex as possible and must sure they include uppercase, lowercase, numbers and symbols.

9. PC's, laptops and smart phones

9.1 The use of laptops is allowed for greater flexibility in working.
9.2 Laptops offer a gateway to BKSConnect, Remote Apps and Home drives via the use of USO and this negates the need for devices to be encrypted
9.3 No data relating to school should be stored locally on any device.
9.4 Staff must not use personal mobile phone devices to access school e-mail accounts through the envelope icon. You can however access your LGfL accounts through the LGfL website by logging in using your username and password.
9.5 Personal mobile devices are not encrypted and could therefore put school data at risk if schools e-mail accounts are accessible via their personal mobile.
9.6 If a breach were to occur due to a personal mobile device being lost or stolen, the school could incur a monetary penalty from the Information Commissioners Office (ICO) and disciplinary action could be taken.
9.7 If staff need to access personal sensitive data through a mobile phone device, Brent Knoll School must provide encrypted mobile devices.

10. Use of E-mail

10.1 Electronic documents containing personal, sensitive or confidential information must be protected just as you would paper documents.
10.2 The schools standard e-mail system is an un-secure email system if sending outside of the school network. It is not intended for the transfer or storage of personal, sensitive or confidential information to other email addresses.
10.3 For example:
10.4 Sending an email which contains personal and/or sensitive information from lewisham.sch.uk to another lewisham.sch.uk or LGfL to LGfL (within the LGfL network) is secure.
10.5 Sending an email which contains personal and/or sensitive information from lewisham.sch.uk to lewisham.gov.uk is not secure.
10.6 The School at present offers 1 secure e-mail account to communicate with other schools which is suitable to transmit personal, sensitive and confidential information which is LGFL mail.
10.7 Brent Knoll Primary School requires that e-mail containing personal, sensitive or confidential information being sent between schools MUST be transferred via the lgfl network.
10.8 Access to any Schools e-mail account may only be done from a Schools approved device or through the LGfL web browser. It is not appropriate to have a school email account attached to a personal mobile through the envelope icon.
10.9 Schools personal sensitive or confidential data must not be sent to personal email accounts to work from home.
10.10 Use of e-mail may be monitored.
10.11 If personal, sensitive or confidential data needs to be sent via email accounts, the data must be included in a word document and sent password protected.
10.12 Any sensitive emails that need to be sent should utilise Egress Switch.

11. Managing Information Systems

11.1 The Server must be located securely and physical access restricted.
- The server operating system must be secured and kept up to date
- Virus protection for the whole network has been installed and will be kept current
- Access by wireless devices will be proactively managed and secured with a minimum of WPA2 encryption

11.2 The Schools Broadband network is protected by a cluster of high performance firewalls provided by LGFL.

11.3 The security of the school information systems and users will be reviewed regularly.

11.4 Virus protection will be updated regularly.

12. Use of removable media including USB sticks

12.1 The term "removable media" refers to any device which holds information electronically other than computers themselves. Principally these will be USB sticks and external hard drives.

12.2 Because of the mobile nature of these devices it increases the risk that schools data could be lost easily.

12.3 Therefore, to minimise the risk of data loss USB sticks and external hard-drives are not permitted for school business. Failure to comply with this could result in disciplinary action or dismissal.

13. Giving Information over the phone

13.1 Staff must ensure that they only give information to people who are entitled to receive it. Do not assume that people are who they say they are. If in doubt, take a phone number and check it before calling back.

13.2 If someone has contacted you in confidence but is not available when you call back it is not appropriate to leave a message with someone else.

13.3 Guard against being overheard when what you are saying is confidential.

14. Using printers and email based faxes

14.1 The use of printers and email based faxes can present a risk that information is wrongly disclosed to unauthorised individuals. For example personal/sensitive data being faxed to the wrong fax number and printed documents being sent to the wrong address due to other documents being picked up at the same time from the photocopier

14.2 Therefore it is important to ensure:
- That you collect your photocopies from the photocopier as soon as you print them
- Do not leave personal, confidential or sensitive information sitting in the photocopy tray
- When collecting your photocopies check to ensure all pages are accounted for and you haven't picked up someone else's documents
- Ensure all photocopiers are cleared down at the end of the working day
- Documents scanned for email based fax correspondence should be cleared out and deleted regularly

14.3 All paper records, whether photocopied or faxed must be managed appropriately. If they contain personal, sensitive or confidential information they must be stored or disposed of securely.

14.4 Only dispose of paper documents containing personal, sensitive or confidential information in confidential waste bins for bulk items. Never use litter bins or recycling bins.

14.5 Small volume disposal of sensitive paper documents should be cross shredded before disposal.

15. Reporting an Information Security Breach

15.1 It is everyone's responsibility to notify a known or suspected data protection/information security breach to their line manager.

15.2 Once the breach is reported, the business manager will contact the school's data protection officer to start the breach investigation process.

15.3 Examples of an information security breach can be (but not limited to):

- Loss or theft of paper records
- Loss or theft of ICT equipment such as a laptop
- Compromised passwords to access the school's network, systems or e-mail
- E-mail sent to the wrong recipient

15.4 If you suspect anything which could compromise school's information you should contact the schools business manager or the schools data protection officer.

16. Who is covered by this policy?

16.1 This policy applies to all school staff, including those employed on a permanent and temporary contract and those who are contracted to work on the schools behalf.

16.2 If you manage staff you must ensure that they have read and understood this and other related policies.

17. What happens if this policy is breached?

17.1 All staff working for or on behalf of Brent Knoll School must read and comply with this policy.

17.2 If you knowingly break or ignore any of the requirements in this policy, the school will take the matter seriously, and may take further action in line with the school's disciplinary procedure.