St John Baptist (Southend) CE Primary School

INFORMATION SECURITY POLICY

Agreed: Nov 2015

Review Date: Nov 2017

By: Curriculum and Pupil Welfare Committee

1. Introduction

This policy covers the handling and security of St John Baptist C of E Primary School information, in electronic or other media (It may sometimes reference to paper).

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

The schools information is valuable information. It must be protected to ensure business continuity, to avoid breaches and meet statutory, regulatory and contractual obligations.

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

3. Who is covered by this policy

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.

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

4. Roles & Responsibilities

Head of School - Caroline Phillips is responsible for:

- Ensuring the application of effective information security measures
- Creating security policies, procedures and guidelines
- Signing off security policies
- Promoting security awareness and ensuring staff understand its importance

Everyone is 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.

5. Training

All schools staff are required to complete basic data protection training and must read, understand and sign off school policies. If you do not understand any part of the schools policies please contact your line manager.

Additional advice and support on information security and data protection matters can be provided by the schools data protection officer at Schoolsdpa@lewisham.gov.uk or call 0208 314 9642.

6. Personal Interest

The school and HR will hold some information about members of staff, other people you may know and/or members of your family. If you would like to see a copy of your own information there is a process that must be followed called 'Subject Access'. (To submit a subject access request please contact your School Business Manager for more information).

Under no circumstances will you inappropriately access information about yourself or other people/your family because they have asked you to. This amounts to unauthorised access to information.

7. Accessing and Retaining information

You should only have access to schools data and systems you need in order to do your job.

You must not keep information longer than is necessary. The school is required to maintain information, regardless of what format it exists in. This means the school and its staff must use proper housekeeping of cupboards, files, folders, computers, systems and mailboxes.

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

- Only access information or systems that you are entitled and authorised to use
- Protect the schools 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 schools retention schedule

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.

8. Keeping information secure

It is the schools duty to protect information on its staff.

The school must comply with the law, including the Data Protection Act.

Any loss of personal, sensitive or confidential information, even if you still have the original or a copy, can have a wide and serious impact. Every case is different although the more information lost the greater the impact could be which could lead to distress/harm to individuals.

A serious loss can damage the school's reputation, hinder its ability to carry out services and lead to an ICO investigation and monetary penalty of up to £500,000.

You must examine the risk of the loss of information you take or send outside the school, assess the impact of such a loss, and mitigate the risks as far as possible.

9. Sharing Information

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.

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.

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

Minimise the data you share as much as possible. Only share what you absolutely must.

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

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.

10. Information at your desk

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.

11. Password Management

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

12. PC's, laptops and smart phones

The use of laptops is allowed for greater flexibility in working but the loss of an un-encrypted laptop that holds schools data is a risk. Therefore, all school mobile devices must be encrypted.

Staff are advised not use personal mobile phone devices to access school e-mail accounts through the envelope icon. 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. It is therefore important that staff ensure they use a 'word' style password if they chose to use personal mobile phone devises to access mail.

You can access your LGfL accounts through the LGfL website by logging in using your username and password.

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.

If staff need to access personal sensitive data through a mobile phone device, the school must provide encrypted mobile devices.

13. Protecting electronic documents

When sending such documents outside of the school they must be protected using secure e-mails or any other school approved solutions.

The School's 'lewisham.sch.uk' e-mail system is not a secure e-mail address and should not be used to share personal/sensitive information unless you are sending to another email address with the same email domain.

For example:

You can send email securely from sch.uk to sch.uk.

You can send email securely from LGfL to LGfL.

14. Use of E-mail

Electronic documents containing personal, sensitive or confidential information must be protected just as you would paper documents.

The schools standard e-mail system is an unsecure system which is not intended for the transfer or storage of personal, sensitive or confidential information.

For example:

Sending an email which contains personal and/or sensitive information from lewisham.sch.uk to another lewisham.sch.uk is secure.

Sending an email which contains personal and/or sensitive information from lewisham.sch.uk to lewisham.gov.uk is not secure.

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.

- LGFL mail (this e-mail account is only secure if you send LGfL to LGfL)

Access to any Schools e-mail account may only be done from a Schools approved device or through the LGfL web browser.

Schools personal sensitive or confidential data must not sent to personal e-mail accounts to work from home.

Use of e-mail may be monitored.

15. Protective marking of information

St John Baptist C of E Primary School requires that e-mail containing personal, sensitive or confidential information being sent between schools is transferred via the LGfL network.

Egress Switch is an option.

16. Use of removable media including USB sticks

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.

Because of the mobile nature of these devices it increases the risk that Schools data could be lost if a device is not encrypted.

To minimise the risk of data loss, no personal/sensitive data will be held on USB sticks unless the USB stick is encrypted. Failure to do so could result in disciplinary action or dismissal.

Please contact the school business manager for approval/authorisation and to have any devices in encrypted.
All use of encrypted removable media will be recorded on an audit log held by the school’s business manager.

Never hold original data on removable storage media. Any loss of data, regardless of whether the storage media is encrypted or not, could result in disruption of business continuity if the data is unavailable.

17. Giving Information over the phone

You must ensure that you 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.

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.

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

18. Using printers and Faxes

The use of printers and 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.

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

When sending faxes, to reduce the risk that information may be breached ensure:

- That you notify the recipient that you are about to send a document
- Confirm with the recipient that they have received the document
- If you receive confidential information ensure your fax machine is in a controlled and secure environment
- Ensure all fax machines are cleared down at the end of the working day.

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.

Only dispose of paper documents containing personal, sensitive or confidential information in confidential waste bins. Never use litter bins.

19. Reporting an Information Security Breach

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

Once the breach is reported, the business manager will contact the schools data protection advisor to start the breach investigation process.

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
- Loss or theft of removable media such as a USB stick
- Compromised passwords to access the schools network, systems or e-mail
- E-mail sent to the wrong recipient
- Receipt of spam or unusual e-mail requesting the recipient to click on a link (please report this immediately to Neil Iles to Lewisham Council)

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

20. What happens if this policy is breached?

All staff working for or on behalf of St Johns Baptist C of E Primary School must read and comply with this policy.

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 schools disciplinary procedure.

Policy Authorisation

Role	Name
Schools Data Protection Officer	Zoe Horsewell
Head of School	Caroline Phillips
Chair of Governors	Andrea Blower