November 2019

Information Security Policy

Adopted by Governors:	26th November 2019
Signed	 Mr F Boulton, Chair of Governors
For review:	September 2021

The School is committed to safeguarding and promoting the welfare of children and expects all staff and volunteers to share this commitment.

BALDWINS GATE CE (VC) PRIMARY SCHOOL

Baldwins Gate CE Primary School

Information Security Policy

1. Introduction

This policy covers the handling and security of Baldwins Gate CE 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. Persons covered by this policy

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

4. Roles and Responsibilities

The head teacher is responsible for:

- Ensuring the application of effective information security measures
- 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 school policies.

6. Personal Interest

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

Under no circumstances will staff inappropriately access information about themselves or others. This amounts to unauthorised access to information.

7. Accessing and Retaining information

Staff should only have access to data and systems needed in order to carry out their role. Information must not be kept for 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. Approved secure disposal methods for paper records and IT kit disposal must be used. Staff must:

- Only access information or systems that they 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

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 school's duty to protect information regarding its staff.

The school must comply with the law, including the General Data Protection Regulation (GDPR) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/

Any loss of personal, sensitive or confidential information, even if the original or a copy is retained, 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.

Staff must examine the risk of the loss of information taken or sent 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 school's work is governed by legislation and therefore this information must be shared for the vital and legitimate interests of the children.

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

Staff should minimise the data they share as much as possible. Staff should only share what they absolutely must.

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

Paper documents should be kept in a secure place and not on view.

10. Information at desks

All staff should keep their working environment clean and tidy in order to practice good records management and should ensure confidential data is kept securely, in a locked cupboard or the school office.

11. Password Management

Effective username and password combinations must be used to avoid unauthorised access to schools systems. Passwords should be as complex as possible; a strong password should include uppercase and lowercase letters, numbers and symbols.

12. PCs, laptops, iPads and smart phones

The use of laptops and iPads is allowed for greater flexibility in working but the loss of an unencrypted 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 school e-mail accounts are accessible via their personal mobile. It is therefore important that staff ensure they use a strong and unique password if they chose to use personal mobile phone devises to access school email.

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.

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 'staffs.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.

14. Use of E-mail

Electronic documents containing personal, sensitive or confidential information must be protected.

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 staffs.sch.uk is secure.

Sending an email which contains personal and/or sensitive information from staffs.sch.uk to a different email domain is not secure.

School's personal sensitive or confidential data must not sent to personal e-mail accounts for any reason.

15. 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.

The mobile nature of these devices increases the risk that School 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.

All use of encrypted removable media will be recorded on an audit log held by the school's business manager.

16. Giving information over the phone

Staff must ensure that they only give information to people who are entitled to receive it. They should not assume that people are who they say they are. If in doubt, a phone number should be taken and checked before calling back.

If someone has contacted the school in confidence but is not available when the call is returned it is not appropriate to leave a message with someone else.

Confidential phone calls should be held in private.

17. Printers and photocopiers

The use of printers and photocopiers can present a risk that information is wrongly disclosed to unauthorised individuals.

Therefore it is important to ensure:

- Photocopies are collected from the photocopier as soon as they are printed
- Personal, confidential or sensitive information is not left on the photocopier
- All pages are accounted for when collecting documents from the photocopier
- No documents are left on the photocopier

All paper records must be managed appropriately. If they contain personal, sensitive or confidential information they must be stored or disposed of securely in accordance with the school's GDPR policy.

18. Reporting an information security breach

It is everyone's responsibility to notify a known or suspected data protection/information security breach, in according with the school's GDPR policy.

Examples of an information security breach include, but are not limited to:

- Loss or theft of paper records
- Loss or theft of ICT equipment such as a laptop
- Compromised passwords to access the schools network, systems or email

- E-mail sent to the wrong recipient
- Receipt of spam or unusual e-mail requesting the recipient to click on a link

If staff suspect anything which may compromise the school's information they should inform the head teacher or data protection officer.

19. Breach of this policy

All staff working for or on behalf of Baldwins Gate CE Primary School must read and comply with this policy.

If staff 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.