Chelwood Nursery School
Chelwood Walk,
London, SE4 2Q

DPO: Georgina Chambers

Information Security Policy

Date Created: 11/05/2018
Date Published:
Doc Ref:
Version 2:

1. Introduction

This policy covers the handling and security of information, in electronic or other media. (It may sometimes reference paper documents)

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

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

Much of our information includes data about school's 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 and governors, including those employed on a permanent and temporary contract and those who are contracted to work on the school's behalf.

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

4. Roles & Responsibilities

- The Data Protection Officer – Georgina Chambers
- The person responsible for ensuring the application of effective information security measures – Louise Karmali (SBM)
- The person responsible for signing off security policies – Nikki Oldhams (HT)
- The person responsible for promoting security awareness and ensuring staff understand its importance – Louise Karmali (SBM)/Nikki Oldhams (HT)

- 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 the basic data protection training and must read, understand and sign off school policies. If you do not understand any part of the school's 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 8183.

6. Personal Interest

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

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.

7. Accessing and Retaining information

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 work.

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

You must not keep information longer than is necessary. You are required to properly maintain all information, regardless of what format it exists in. This means you 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 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

  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 on its staff.

The school must comply with the law, including all relevant data protection legislation.

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 and the more information lost the greater the impact 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 €20,000,000.

When working with personal, sensitive or confidential information you are required to assess the risk of the likelihood of the loss of information occurring and the impact that any loss would have.

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 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 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.

You must use secure ways to transfer Schools information that contains personal, sensitive or confidential data. See the following sections of this policy:

- Protecting electronic documents
- Use of e-mail
- Use of removable media including USB sticks
- Sending information by post

10. Protective marking of information

The School requires that e-mail containing personal, sensitive or confidential information being sent between schools is transferred via the LGfL network.

If personal, sensitive or confidential data needs to be sent via sch.uk accounts, the data must be included in a word document and sent password protected.

11. 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

12. Carrying paper documents away from the office

If you need to transport paper documents containing personal, sensitive or confidential information away from School premises you must make every effort to protect it. Principle 6 of the General Data Protection Regulation states data must be securely protected.

You must assess the risks and take effective actions to protect the information. This can include:

- Keeping the number of documents to an absolute minimum
- Use a lockable bag
- Keep documents out of sight and never unattended (left in car for example)
- Where possible, keep documents in a secure location when away from the office
- Use loose leaf note pads so that you do not carry old or unnecessary information
- Always keep a record of the information you are taking and record when it is returned

In the event that you are aware paper documents are lost or compromised you must contact your line manager as early as possible. The schools breach process must then be followed.

13. Password Management

Effective username and password combinations must be used to avoid unauthorised access to school's systems. Make passwords as complex as possible and must sure they include uppercase, lowercase, numbers and symbols. Change passwords regularly, every 30-90 days.

14. PC's, laptops and smart phones

The use of laptops is allowed for greater flexibility in working.

All school mobile devices must be encrypted.

Staff must not use personal mobile phone devices to access school e-mail accounts.

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.

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.

In any other circumstance, if staff need to access personal sensitive data through a mobile phone device, the School must provide encrypted mobile devices.

15. Protecting electronic documents

When sending 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. Where possible use LGFL mail

16. 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 insecure 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.

Any email which contains personal and/or sensitive to the local authority or other schools must be sent by secure e-mail accounts such as Egress to communicate with other schools as this is suitable to transmit personal, sensitive and confidential information.

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

When sending personal, sensitive or confidential content you are required to protectively mark the e-mail (see 11. Protective Marking of Information)
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.

17. 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.

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

If you need to use a USB stick, this must be approved by the school’s business manager who will provide you with a schools encrypted stick.

Under no circumstances will staff use their own personal USB sticks for school’s official business.

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.

18. 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.

19. 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
- That you 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
- 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
- You 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
- 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.

20. 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 school's data protection officer 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 Lewisham Council)

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

21. What happens if this policy is breached?

All staff working for or on behalf of the 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 school's disciplinary procedure.

The school will contact the Police if there is evidence that someone has deliberately broken the law.

Please refer to the Data Breach Process for full details of how to report breaches.

22. Policy Authorisation

Role	Name
Data Protection Officer	Georgina Chambers
Schools Business Manager	Louise Karmali
Head Teacher	Nikki Oldhams
Governors	Stella Jeffrey