Lainesmead Primary School and Nursery

Confidentiality Policy

Approved by Governors: January 21

Next review: January 23

Signatures

Subject Co-ordinator	**Sarah Ellison**
Headteacher	**Eirian Painter**
Chair of Governors	**Alan Mulrooney**

Confidentiality Policy

Introduction

Staff working at Lainesmead Primary School and Nursery have access to a variety of information that must be regarded as confidential.

This policy applies to all staff employed by the school, including temporary, voluntary and agency staff. It also applies to governors, volunteers, visitors on work experience placements and parent helpers.

Types of confidential information
Information that is regarded as confidential can relate to:

A variety of people e.g.
- pupils
- parents
- staff/colleagues
- governors
- job applicants.

A variety of matters e.g.
- home addresses & telephone numbers
- conduct and performance
- performance and development reviews/performance management
- health/medical records
- pay and contracts
- references
- internal minutes, memos etc.
- confidential budgetary or policy information
- other personal information

These lists are not exhaustive but will extend to cover any other information of a sensitive nature relating to employees, pupils and others connected with the school and to the work of the school itself.

Potential recipients of information
Within the course of daily operation, information related to the school, or those connected to the school, may be requested by, or supplied by, or passed to a range of people.

This might include:
- internal colleagues (teachers, support staff, governors)
- colleagues in other schools
- management teams
- pupils
- governors
- trade unions/professional associations
- parents
- partner organisations (LA, DfE, Teachers' Pensions)
- other external organisations
- the public
- the press
- contractors/potential contractors

Great care must be taken by both the recipient and the supplier of information to ensure that it is dealt with appropriately and in a sensitive manner.

Particular responsibilities

 If someone requesting information is not known to staff, particularly in the case of telephone calls, their identity and the legitimacy of their request should be verified by calling them back. A person with genuine reasons for seeking information will never mind this safety measure.

 Wherever possible, a response to requests for information should only be given when the request has been made in writing e.g. employee references.

 The same principle applies when sending emails and faxes. Staff should always check that the information is going to the correct person and is marked confidential where appropriate.

 Being known as an employee of the school may mean being asked for information about a member of staff. People requesting this information must be informed that employees are unable to discuss confidential school matters including staff members.

Persistent enquiries should be referred to the Head Teacher or School Business Manager.

 The General Data Protection Regulations Act refers to the principle of third party confidentiality. Information relating to, or provided by, a third party should not be released without the written consent of the third party or unless an order for disclosure is made by a court of competent jurisdiction. Where they are unsure what to do, staff should refer the matter to the School Business Manager, for guidance.

The form confidential information can take:

Confidential information can take various forms and be held and transmitted in a variety of ways, e.g.

 manual records (files)

 computerised records, disks and memory sticks

 written reports/minutes/agendas/file notes etc

 letters and messages

 telephone calls

 face-to-face

 Email

 internet/intranet

The methods of acquiring information can also vary.

Individuals and groups may become aware of confidential information in the following ways:

 access is gained as part of the employee's day to day work

 information is supplied openly by an external third party

 employees may inadvertently become aware of information

 information may be disclosed

Particular responsibilities

 Employees should be aware that they may have disclosed to them sensitive information in the course of their work or outside of school. In some circumstances the individual may request that the information remains confidential.

 Staff will also need to be aware that they may be obliged to disclose certain information e.g. relating to child protection issues and should make it clear to the individual either that confidentiality cannot be guaranteed and/or direct them to a more appropriate officer or decline to receive the information. Employees should use their discretion regarding these matters, should refer to appropriate procedures and, if in doubt, should seek advice from the Head teacher.

Responsibility of individuals in possession of sensitive information
All information received in the course of employment, no matter how it is received, should be regarded as sensitive and confidential. While it is often necessary to share such information, in doing so, employees should consider the following key points.

The nature of the information:
 how sensitive is it?
 how did it come to your attention?

The appropriate audience:
 who does the information need to be shared with?
 for what purpose?
 who is the information being copied to? Why?
 does restriction of access need to be passed on to your audience?

The most appropriate method of communication:
 verbal
 written
 email
 in person

The potential consequences of inappropriate communication.
It is also an individual employee's responsibility to safeguard sensitive information in their possession.

Particular responsibilities
Sensitive information should be kept secure.
 Filing cabinets should be kept locked when unattended.
 Child protection information is kept in a separate, secure filing cabinet.
 Sensitive information should not be left on desks or photocopiers/printers.
 Papers should not be left lying around at home or in the car. If confidential materials or paperwork are taken out of the office, precautions must be taken to ensure that they are not accessible to third parties.
 Appropriate steps should be taken to keep track of files which are on loan or being worked on i.e. a record of the date sent and the recipient's name and position.
 If it is necessary to supply personal files through the external mail, this must be sent by recorded delivery.
 Copies of emails should be stored securely.
 Steps should be taken to ensure that private/confidential telephone calls/conversations are not overheard.
 Meetings where sensitive or confidential information is being discussed should be held in a secure environment.
 Confidential paperwork should be disposed of correctly either by shredding it or using the confidential waste bin.
 Personal data should not be used for training or demonstration purposes where fictitious data can be used.

2. Computer data should not be left exposed to others' view when unattended.
 Screens should be "locked" and
 Screen savers should be used when computers are unattended.
 Machines should be switched off over night.

Computer files should be kept securely

 Passwords should be used and these should not be disclosed to colleagues unless absolutely necessary.

 Passwords should be changed periodically (at least every 6 months).

 Sensitive data should not be stored on public folders.

 Staff should be familiar with the security of Email/internet systems.

 Staff should use the school email service for all school related emails

 Access to individual's computers should be restricted.

 Any user Ids and passwords used for the internet should remain confidential.

 All work carried out on a computer should be stored safely either in a personal directory, or onto a memory stick or portable hard drive which should be kept securely.

A variety of phrases may be used on correspondence to denote confidentiality. As a general rule:

 Post marked 'personal' or 'for the attention of the addressee only' should only be opened by the addressee personally;

 Post marked 'private' and/or 'confidential' may be opened by those responsible for distributing the post within the school.

Confidential mail which is then forwarded internally should continue to carry a confidential tag.

Other responsibilities

 Employees should have regard to potential difficulties which may arise as a result of discussions outside work. Staff should be cautious about discussing specific and sensitive matters and should take steps to ensure that information is not passed on.

 Personal (e.g. home addresses and telephone numbers) and work-related information (e.g. salary details, medical details) relating to individuals, should not be disclosed to third parties except where the individual has given their express permission (e.g. where they are key holders) or where this is necessary to the particular work being undertaken, e.g. it is necessary for an individual to be written to.

 The Head teacher should comply with the procedures for the storage and sharing of information relating to individuals' Performance Management Appraisal Reviews.

 Personal files should not normally be shared with third parties other than the Head teacher who is responsible for writing references. Exceptions may apply in the case of legal proceedings.

Employees should use their discretion in these matters and if in doubt, should seek advice from the Head teacher.

The consequences of revealing confidential information without authority:

Staff should ensure that they are familiar with this Confidentiality Policy and the GDPR Policy. While there is an expectation that staff will use their professional discretion in applying the policy, they should always seek advice from the Head teacher where they are unsure.

Staff should be aware that serious breaches of the Confidentiality Policy may result in disciplinary action being taken. The severity of the sanction will be assessed with regard to the potential harm the disclosure will have caused to the individual concerned. Some breaches of confidentiality could be regarded as potential serious or gross misconduct that could result in dismissal.