HUNDON AND THURLOW PRIMARY FEDERATION

Laying the foundations for a bright future

The Parable of The Wise and The Foolish Man
(Matthew, Chapter 7, verses 24 to 27 and the Gospel of Luke, Chapter 6, verses 46 to 49)

CONFIDENTIALITY POLICY

NB: This policy has been discussed and considered for equality giving consideration to the protected characteristics- gender, age, race, disability, religion or belief, sexual orientation, gender reassignment, pregnancy or maternity and any other recognised area of discrimination.

Reviewed: Summer 2022

Date of review: Spring 2024

Approved by Finance and Personnel Committee

Signature of Chair of Governors:

Signed: **Chair of Governors**

Working in Hundon and Thurlow Primary Federation necessarily means having access in a variety of ways to information that may 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.

Rationale

The safety, well-being and protection of our pupils are the paramount considerations in all decisions staff, at this school, make about confidentiality. The appropriate sharing of information between school staff is an essential element in ensuring our pupils' well-being and safety. It is an essential part of the ethos of our school that trust is established to enable pupils, staff, and parents/carers to seek help both within and outside the school. We, therefore, minimise information sharing to those occasions which are appropriate to ensure pupils and staff are supported and safe. Pupils, parents/carers and staff need to know the boundaries of confidentiality in order to feel safe and comfortable in discussing personal issues and concerns. The school's attitude to confidentiality is open and easily understood and everyone should be able to trust the boundaries of confidentiality operating within the school. Everyone in the school community needs to know that no one can offer absolute confidentiality and that there are limits of confidentiality that can be offered by individuals within the school community - so they can make informed decisions about the most appropriate person to talk to.

Definition of Confidentiality

The dictionary definition of confidential is "something which is spoken or given in confidence, private, and entrusted with another's secret affairs". When speaking confidentially to someone, the confider has the belief that the confidant will not discuss the content of the conversation with another. The confider is asking for the content of the conversation to be kept secret. Anyone offering absolute confidentiality to someone else would be offering to keep the content of his or her conversation completely secret and discuss it with no one. In practice there are few situations where absolute confidentiality is offered. We have to strike a balance between ensuring the safety, well-being and protection of our pupils and staff, ensuring there is an ethos of trust where pupils and staff can ask for help when they need it - and ensuring that when it is essential to share personal information, child protection procedures and good practice are followed. This means that in most cases what is on offer is limited confidentiality. Disclosure of the content of a conversation could be discussed with professional colleagues but the confider would not be identified except in certain circumstances. The general rule is that staff should make clear at the beginning of the conversation that there are limits to confidentiality. These limits relate to ensuring children's safety and well-being.

Types of confidential information

Information that is regarded as confidential can relate to a variety of people:

- Pupils
- Parents
- staff/colleagues
- governors
- job applicants

A variety of matters:

- home addresses & telephone numbers
- conduct and performance

- performance & development review/performance management
- health/medical
- 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 in a sensitive manner.

Specific responsibilities

If someone requesting information is not known to staff, particularly in the case of telephone calls, his/her identity and the legitimacy of his/her 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. 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, for instance, by parents about a member of staff who is off sick. Although this can be awkward, parents must be informed that employees are unable to discuss confidential school matters. Under GDPR guidance there is no requirement to disclose the name of a colleague who has tested positive for COVID 19, either to other staff or parents. Use of a "no names" protocol should be adopted, unless permission is sought from the individual for their details to be shared.

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. Any request to share information should be considered using the flowchart attached to this policy and full completion of the Data Sharing decision form (Appendix 1).
All personal information, and in particular sensitive personal information and confidential information should be encrypted before being sent by email, or sent by recorded delivery. You may not send such information by fax unless you can be sure that it will not be inappropriately intercepted at the recipient fax machine.

- 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 and for what purpose? Who is the information being copied to and why? Does restriction of access need to be passed on to your audience?
- The most appropriate method of communication. Verbal, written. Email or 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 the photocopier/fax/printer.
- You should not take confidential or other information home without prior permission of the Headteacher, and only do so where satisfied appropriate technical and practical measures are in place within your home to maintain the continued security and confidentiality of that information. Papers should not be left lying around at home or in the car. If confidential materials or paperwork are taken out of the office, you must ensure that:
    a) The information is kept in a secure and locked environment where it cannot be accessed by family members or visitors; and
    b) All confidential material that requires disposal is shredded or, in the case of electronic material, securely destroyed, as soon as any need for its retention has passed. Please see the Online Safety Policy for further information.
- 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 faxes and Emails should be stored securely.
- Steps should be taken to ensure that private/confidential telephone calls/conversations are not overheard, paying particular attention to this if working from home.
- 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.
- Personal data should not be used for training or demonstration purposes where fictitious data can be used.
- Where the use of Zoom or Microsoft Team's technology is adopted, consider carefully the guidance within the online safety policy regarding recording the meetings.

Computer data should not be left exposed to others' view when unattended.

- Password protected screen savers should be used when computers are unattended. Staff should be aware that if they fail to log off and leave their terminals unattended they may be held responsible for another users activities on their terminal which may breach this policy, the Data Protection Policy and the requirement for confidentiality in respect of certain information.
- Machines should be switched off over night.

Computer files should be kept securely.

- Passwords are unique to each user and staff are required to select a password which contains at least 8 characters including numbers, letters and/or special characters. All passwords should be considered complex. Passwords should not be disclosed to colleagues unless authorised by a member of SLT.
- Passwords should be changed periodically (at least every 3 months), not be obvious or easily guessed (e.g. birthdays or other memorable dates, memorable names, events or places etc.).
- You should not write down passwords if it is possible to remember them, if necessary, you may write down passwords as long as you store them securely (e.g. in a locked drawer)
- 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. You may connect your own devices (including but not limited to smartphones, tablets, and laptops) to the schools Wi-Fi provided that you follow the requirements and instructions governing this. All usage of your own device whilst connected to the school network is subject to all relevant school policies.
- 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 an encrypted memory stick or portable hard drive which should be kept securely.
- You should not store data on any mobile device.
- Computer files should backed up regularly and not solely saved to the hard disk.

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. While it is natural (and indeed can be therapeutic) to talk about work at home or socially, staff should be cautious about discussing specific and sensitive matters and should take steps to ensure that information is not passed on. Staff should be particularly aware that many people have a direct interest in education and schools and even close friends may inadvertently use information gleaned through casual discussion.
- 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 Headteacher should comply with the procedures for the storage and sharing of information relating to individuals' Performance Management Appraisal Reviews.
- Personal and case files should not normally be shared with third parties other than the Deputy Head teacher and those 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 Headteacher.

The consequences of revealing confidential information without authority

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

Staff should be aware that serious breaches of the 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 potentially serious or gross misconduct that could result in dismissal.

Confidentiality Agreement

I, the undersigned, hereby agree that I will at all times, whether or not in the employment of this School and except where such information is in the public domain:

- maintain the strictest confidentiality with regard to the affairs of the school and its pupils, parents, suppliers and employees, except to the extent that I may be authorised to disclose them by the governing body, a court of law, any authorised or enforcement agency (such as the police) or by public interest disclosure legislation;
- refrain from revealing or using confidential information and/or data for personal gain.

I undertake to familiarise myself with the data protection procedures set down by the school as a result of the General Data Protection Regulation and understand that the school is obliged as a consequence to view any breach of these procedures as a serious matter of discipline.

I understand that any breach of this agreement could result in the school's sensitive and confidential data being disclosed and any such conduct on my part may render me liable to summary dismissal under the disciplinary procedure.

Name: _____

Signature: _____

Date: _____

Appendix 1 Data Sharing Decision Form

Name of Organisation	
Name and position of person requesting data	
Who will have access to data within organisation	
Date requested	
Purpose of request and objective of data sharing	
Lawful basis for sharing – please state which	
Why is sharing necessary	
Are additional conditions met for special category data (where applicable)?	
Decision and reason for disclosure or non-disclosure of information	
Decision taken by (name and position)	
Date of disclosure	
What arrangements are there for complying with individuals' information rights?	
How is data supplied i.e. encrypted, secure email, secure postal delivery, by hand	
Agreements made regarding data retention/deletion by organisation	
Signed	
Dated	

FLOWCHART OF HOW AND WHEN TO SHARE INFORMATION