Mighty Oaks Academy Trust

Staff Confidentiality Policy

Policy in effect from: September 2023

Review Date: September 2025

Contents:

Statement of intent

This document guides staff, volunteers and visitors on the policy and procedures surrounding confidentiality.

This policy will be adhered to at all times by staff, volunteers, visitors, pupils and parents. In order to ensure the utmost level of safety for pupils, staff members at the school have a duty to act in accordance with this policy and not share information with external agencies, other schools or individuals.

The Staff and Volunteer Confidentiality Policy has the following benefits:

- Ensures that important information regarding the school is not shared
- Guarantees that financial information stays confidential and secure
- Helps to build trust amongst staff, volunteers and external agencies
- Supports the school's safeguarding measures

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Crime and Disorder Act 1998
- Equality Act 2010
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Education Act 2002
- Human Rights Act 1998
- The Education (Pupil Information) (England) (Amendment) Regulations 2019
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2018) 'Information sharing'
- DfE (2018) 'Working Together to Safeguard Children'

This policy is compliant under the following case law:

- The Common Law Duty of Confidentiality

This policy operates in conjunction with the following school policies:

- Data Protection Policy
- Disciplinary Policy and Procedure
- Records Management Policy
- Child Protection and Safeguarding Policy
- Anti-bullying Policy
- Freedom of Information Policy
- Whistleblowing Policy
- Online Safety Policy

2. Definitions

For the purposes of this policy, "**confidentiality**" is an understanding that any information shared with someone in confidence will only be passed on to a third party with the prior and explicit agreement of the person disclosing it.

A "**disclosure**" is the sharing of any private information; this term does not solely relate to child protection issues.

The term "**limited confidentiality**" refers to the disclosure of information with professional colleagues; however, the confider would not be identified except in pre-determined circumstances.

3. Roles and responsibilities

The Head of School will:

- Ensure staff understand why they must agree to the regulations set out in this policy and the documents outlined in the legal framework.
- Ensure that staff members receive briefings on confidentiality.
- Remain informed of any confidentiality, safeguarding or data protection concerns within the school.
- Decide on the appropriate disciplinary procedures that will be placed upon any staff member who is in breach of their confidentiality agreement or otherwise withholds, discloses, or shares confidential information without reason.
- Ensure that this policy is kept up-to-date with all other documents, policies and statutory frameworks which operate in conjunction with this policy.

The DPO will:

- Address all concerns relating to data protection.
- Provide advice in the event of a data breach.
- Understand all relevant legislation including the Data Protection Act 2018 and the UK GDPR.
- Understand how to correctly withhold, store, move and share data.
- Ensure that the school's data is protected at all times and react quickly to any vulnerabilities.

The DSL will:

- Understand the importance of information sharing with other schools, safeguarding partners, practitioners and any other relevant agencies or organisations.
- Understand relevant data protection legislation and regulations with particular reference to the Data Protection Act 2018 and the UK GDPR.
- Keep detailed, accurate, secure written records of concerns and referrals and understand the purpose of record-keeping.

All staff members, volunteers and individuals working in cooperation with the school will:

- Uphold their responsibility and duty in relation to confidentiality.
- Ensure that information and personal details are not shared or discussed with others, except for the appropriate necessary bodies.
- Keep information regarding the school, including its pupils and parents, confidential.
- Be briefed on confidentiality in line with the Code of Conduct and, where necessary, a responsible use of ICT agreement.

4. Confidentiality and child protection

The school will always prioritise the welfare of its pupils and this will remain the primary concern when investigating an allegation which has been made against a member of staff.

A staff member who faces allegations relating to safeguarding concerns may find the investigation process extremely stressful. For this reason, the school will ensure that anyone who holds information relating to the investigation keeps said information confidential and that it will not ordinarily be shared with any other staff, pupils or parents who are not involved in the investigation.

The processes involved in maintaining confidentiality and carrying out an investigation will operate in line with The Education Act 2011, which made the publishing of any material illegal if it leads to the identification of a staff member in a school who has been subject to allegations by, or on behalf of, a pupil in the school.

The school will take steps to ensure that confidentiality is maintained against any unwanted publicity whilst an allegation is being investigated or considered; this will include ensuring that all staff who have access to files and data, or any other relevant form of information, sign a confidentiality agreement.

The school will ensure that the above restrictions on sharing information (including any speech, writing, or other communication which is exposed to any section of the public) are adhered to and will apply until:

- The accused person has been charged with a relevant offence.
- The Secretary of State publishes information about an investigation or decision in a disciplinary case arising from the allegation.

These restrictions will not be applied under the following circumstances:

- The individual who is being investigated waives their right to anonymity by going public on their own accord
- The individual being investigated provides written consent for another individual to publicly disclose the relevant confidential information
- A court lifts the reporting restrictions in response to a request to do so

Any individual, such as a parent or staff member, who discloses information to any section of the public, e.g. on a social networking site, will be in breach of the reporting restrictions if what they have disclosed could lead to the identification of the staff member by members of the public.

All external visitors will be made aware of this policy and act in accordance with it when dealing with information, particularly sensitive information, regarding the school, its pupils and parents.

The Head of School will be informed of all incidents regarding child protection concerns which are highlighted by a volunteer, parent or another external party to the school.

Staff members will **immediately** inform the DSL of any concerns regarding a pupil's safety or welfare. Any concerns raised over a child's welfare and safety will be reported immediately to ensure that any intervention necessary to protect the child is accessed as early as possible.

Staff members will not be obliged to inform the police on most matters relating to illegal activity, such as illegal drugs or assaults. These will be assessed on a case-by-case basis with the support of the SLT.

5. Sharing information

The school will take the stance that all information about individual pupils is private and should only be shared with other professionals who have a legitimate need to know.

Under no circumstances will personal information about pupils, staff members or the school be passed on indiscriminately.

Under no circumstances will information regarding the school's finances be shared with anyone, other than those with a legitimate need to know.

If members of staff, volunteers or cooperating external parties share unsuitable or misrepresented information, the school holds the right to take the appropriate civil, legal or disciplinary action.

All staff and volunteers will report safeguarding concerns to the DSL as soon as possible and in an appropriate setting.

All data will be processed and held in line with the school's Data Protection Policy. In the event of information and data being shared with external or inappropriate parties, the situation will be dealt with in accordance with the Data Protection Policy.

The DSL will recognise and assure staff members with concerns about a safeguarding issue that the Data Protection Act 2018 and the UK GDPR do not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare.

Staff members who manage or have access to the school's data will always uphold the school's obligation to process personal information fairly and lawfully, and keep the information they hold safe and secure.

The school will be open and honest with all individuals about how and why data is shared, unless it is unsafe to do so.

Only information that is necessary for the purpose it is being shared for will be shared.

All decisions and reasons for sharing data will be recorded by the DPO.

6. Breaking confidentiality

When confidentiality must be broken because a child may be at risk of harm, in accordance with the school's Child Protection and Safeguarding Policy, the school will ensure the following:

- Pupils will be told when information has been passed on
- Pupils will be kept informed about what will be done with their information
- To alleviate their fears concerning the information becoming common knowledge, pupils will be told exactly who their information has been passed on to

If confidential information is shared with the explicit consent of the individuals involved, and they are informed of the purpose of sharing the information in question, there will be no breach of confidentiality or of the Human Rights Act 1998.

In the event that explicit consent for sharing confidential information is not gained, an individual will satisfy themselves that there are reasonable grounds to override the duty of confidentiality in these circumstances before sharing the data.

The school will recognise that overriding public interest is a justifiable reason to disclose information; however, permission from the headteacher will be sought prior to disclosing any information regarding the school.

Staff will act in accordance with the school's Whistleblowing Policy at all times.

Staff in breach of this policy may face disciplinary action if it is deemed that confidential information was passed on to a third party without reasonable cause.

7. Responsible use of ICT and technology

Every member of staff will adhere to the school's ICT Acceptable Use Policy at all times.

All staff, with particular reference to ICT technicians and staff members with access to wider files and data, will understand their obligation to use ICT systems in a responsible way and respect others' privacy and confidentiality.

Staff will understand that their use of ICT systems, email and other digital communications will be monitored and the staff responsible for monitoring such activities will not share any confidential information unless this is for the purposes of keeping children safe or any other legal complication.

Staff will never disclose their password to anyone, nor will they attempt to use another individual's account details.

All staff will immediately report illegal, inappropriate, or harmful material seen on another individual's network to the Head of School.

Anyone found accessing, copying, removing or altering any other user's files without permission will face appropriate disciplinary measures.

Communication with pupils and parents will only take place through official school systems.

The Head of School and DPO will be informed immediately in the event of a data breach on any school device.

The use of any programmes or software that attempts to bypass filtering or security systems in place at the school is strictly prohibited.

As outlined in the school's Data Protection Policy, all staff members will understand that any staff or pupil data, which they have access to, will be kept private and confidential unless the sharing of information is deemed necessary as outlined above.

8. Management and security of school records

In line with the school's Records Management Policy, any staff member who is responsible for or has access to files, documents or data within the school's ICT infrastructure, database or other, is contractually obliged to maintain the security and management of such records which relate to:

- Pupils
- School management

- Finances
- Personal details of pupils or staff
- Information regarding progress and attainment which is not published on the school website

9. Maintaining confidentiality when staff leave

The school expects the departing staff member to respect and maintain any confidential information once they have left the school's employment, as per the privacy and confidentiality terms within their contract of employment.

The school will not share any information that is held on the departing staff member, unless they have an obligation to do so or we have obtained consent – this will be detailed in a privacy notice, which will be available on the school's website.

Where necessary, for example in the case of highly sensitive information, a settlement agreement will be established to ensure confidentiality – the departing staff member and Head of School will agree and sign this agreement.

All data that the school retains on the departing staff member will be stored in accordance with the Data Protection Policy and Records Management Policy.

Where consent was used to obtain information and the departing employee wishes to withdraw consent, they will express this to the DPO in writing.

Where the departing staff member had access to any password protected sensitive data, e.g. school bank accounts, the passwords will be changed upon their departure.

10. Monitoring and review

This policy will be monitored for effectiveness by the Chief Operations Officer and Executive Leader / CEO and is reviewed every two years, or where necessary in light of changes to the law or statutory guidance, or breaches/incidents.

All changes will be communicated to relevant stakeholders.

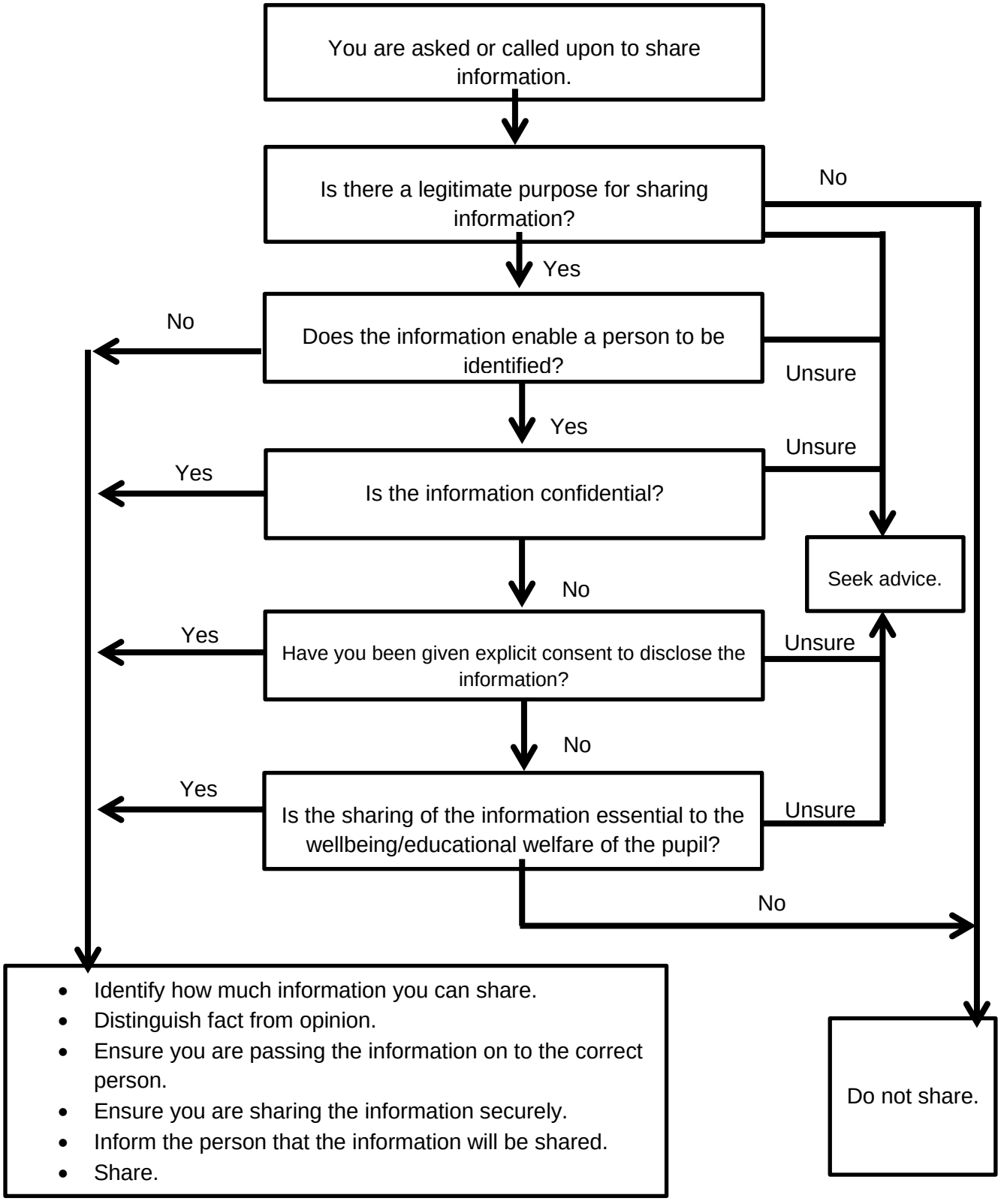
A record of information which has been shared will be continuously kept up-to-date.

This record will state the premise of the information, whom it was shared with and the purpose for sharing it.

The record will be kept on The School Bus and can be accessed by all appropriate staff members.

On an annual basis, the Head of School and DSL will review the record to ensure that all reasonable measures to safeguard pupils and protect the reputation of the school are being taken.

Information Sharing Flowchart



Notes

- If there are child protection concerns, follow the relevant procedures without delay.
- Always seek advice if you are unsure whether to share information.

Staff Exit Procedure Checklist

Use this checklist to ensure that all duties regarding the departure of a staff member have been completed prior to the end of their notice period.

Employee's name	
Job role	
Date resignation notice letter was received	
Last day	
Person responsible for overseeing their exit	

Action	Complete (Y/N)?	Date completed
Once the employee has handed in their notice, the Head of School acknowledges it in writing within one week.		
Begin the recruitment process, if appropriate.		
The Head of School informs the relevant staff, e.g. HR departments.		
The HR provider provides the departing staff member with a leavers letter, specifying essential information relating to the staff member's exit, e.g. their final day and any holiday entitlements.		
The Line Manager organises the exit interview, giving the departing staff member at least one week's notice.		
The Line Manager of writes the exit interview questions.		
A copy of the exit interview questions is sent to the departing staff member.		

Action	Complete (Y/N)?	Date completed
If the departing staff member declines the interview, they are asked to complete the questions as a questionnaire and send it back to the Line Manager.		
A handover period is established, if necessary.		
The COO manager and DPO establish what information the school needs to keep pertaining to the departing staff member, who is informed of this.		
The COO manager ensures the ICT technician terminates the departing staff member's accounts at the school and obtains any school-owned equipment.		
The COO manager ensures business continuity by: • Removing the departing staff member from the website and any contact lists. • Delegating the departing staff member's duties until a replacement is found. • Ensuring any repayments are made to either party, e.g. travel expenses.		
The COO manager arranges for someone to fulfil any additional roles that the departing staff member has, e.g. fire safety officer or first aider.		
The COO manager establishes a system for incoming emails to the departing staff member's account, e.g. forwarded to another staff member automatically.		
HR systems are updated, e.g. payroll.		
Colleagues and the school community are informed of the staff member's departure, adhering to confidentiality issues.		
The exit interview is held at least one week before the departing staff member's final day.		
The Head of School makes arrangements to handle issues raised from the exit interview.		

Action	Complete (Y/N)?	Date completed
Where the departing staff member had access to password protected sensitive data, e.g. bank accounts, the COO manager changes the passwords upon their departure.		
Where necessary, an information settlement agreement is established.		