



Staff and Volunteer Confidentiality Policy

Reviewed by:	Anna Yates
Date reviewed:	1 st September 2026
Next review date:	1 September 2027
Version:	1

Contents:

Statement of intent

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Confidentiality and child protection
5. Sharing information
6. Breaking confidentiality
7. Responsible use of ICT and technology
8. Management and security of school records
9. Maintaining confidentiality when staff leave
10. Monitoring and review

Appendices

- A. Information Sharing Flowchart
- B. Staff Exit Procedure Checklist

Statement of intent

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

The school recognises that safeguarding and promoting the welfare of children is everyone's responsibility. Confidentiality must never be used as a barrier to sharing information where this is necessary to safeguard or promote the welfare of a child. Staff, volunteers and visitors must understand that information should be shared appropriately, proportionately, securely and without delay where there is a safeguarding concern.

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 Burscough Village Primary 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

Legal framework

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

- Crime and Disorder Act 1998
- Equality Act 2010
- Human Rights Act 1998
- Education Act 2002
- Children Act 1989
- Children Act 2004
- Counter-Terrorism and Security Act 2015
- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- The Education (Pupil Information) (England) (Amendment) Regulations 2019
- DfE (2026) 'Keeping children safe in education'
- DfE (2024) 'Information sharing: advice for practitioners providing safeguarding services'
- DfE (2026) 'Working Together to Safeguard Children'
- DfE guidance on meeting digital and technology standards in schools and colleges, including filtering and monitoring standards
- DfE guidance on generative artificial intelligence in education, where relevant to school systems and practice

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
- Allegations of Abuse Against Staff Policy

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.

1. Roles and responsibilities

The headteacher is responsible for:

- Ensuring staff understand why they must agree to the regulations set out in this policy and the documents outlined in the legal framework.
- Ensuring that staff members sign confidentiality agreements.
- Remaining informed of any confidentiality, safeguarding or data protection concerns within the school.
- Deciding 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.
- Ensuring that this policy is kept up-to-date with all other documents, policies and statutory frameworks which operate in conjunction with this policy.
- Ensuring that the school’s confidentiality arrangements support the requirements of Keeping children safe in education 2026, Working Together to Safeguard Children and relevant DfE information sharing guidance.
- Ensuring that all staff and volunteers understand that they must not promise absolute confidentiality to pupils, parents or carers where safeguarding concerns arise.
- Ensuring that staff know how to report concerns promptly to the DSL or deputy DSL and understand that anyone can make a referral to children’s social care where there are concerns about a child’s welfare or safety.

The DPO is responsible for:

- Addressing all concerns relating to data protection.
- Providing advice in the event of a data breach.
- Understanding all relevant legislation including the DPA 2018 and the UK GDPR.
- Understanding how to correctly withhold, store, move and share data.
- Ensuring that the school’s data is protected at all times and react quickly to any vulnerabilities.

The DSL is responsible for:

- Supporting staff and volunteers to understand when and how to share safeguarding information.
- Ensuring that child protection files and safeguarding records are accurate, secure, detailed and shared appropriately when children move schools or where information is required by safeguarding partners.
- Liaising with children's social care, police, health services, Family Help services, other education providers and relevant agencies where information sharing is necessary to safeguard or promote the welfare of a child.
- Reminding staff that data protection legislation does not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare.
- Seeking advice from the DPO, safeguarding partners or relevant statutory services where there is uncertainty about information sharing, while ensuring that advice-seeking does not cause delay where a child may be at risk.

All staff members, volunteers and individuals working in cooperation with the school are responsible for:

- Upholding their responsibility and duty in relation to confidentiality.
- Reading and understanding Part One of Keeping children safe in education 2026 as required by the school.
- Maintaining an appropriate level of confidentiality by only involving those who need to be involved, such as the DSL, deputy DSL, children's social care or police.
- Never promising a pupil or family that information will be kept secret where this may not be in the child's best interests.
- Reporting safeguarding concerns immediately and sharing all relevant information with the DSL or deputy DSL.
- Recording concerns accurately, using the child's own words where possible, and following the school's agreed recording system.
- Understanding that fear of sharing information must not be allowed to stand in the way of safeguarding and promoting the welfare of children.
- Sharing information securely and only with those who have a legitimate need to know.
- Understanding and signing a confidentiality agreement and, where necessary, a responsible use of ICT agreement.

2. 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, and will always follow the procedures set out in the Allegations of Abuse Against Staff Policy.

Where a child makes a disclosure, staff must listen carefully, reassure the child that they have done the right thing by speaking, avoid making promises of confidentiality, avoid investigating or asking leading questions, and report the concern to the DSL or deputy DSL without delay. Staff should explain, in an age-appropriate way, what will happen next and who the information will need to be shared with, unless doing so would increase risk to the child or another person.

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 school will maintain confidentiality during safeguarding enquiries, allegations or low-level concerns involving adults, including supply staff, volunteers, contractors and governors. Information will only be shared with those who need to know in order to safeguard children, manage risk, meet statutory duties or support a fair and appropriate process.

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 headteacher 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, and where necessary the LA designated officer. 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.

3. Sharing information

The school recognises the importance of timely and effective information sharing in safeguarding children. No single practitioner can have a full picture of a child's needs and circumstances. Staff must share information where this is necessary to help identify concerns, support early help or Family Help, protect children from harm, or contribute to statutory assessments and multi-agency safeguarding work.

Data protection legislation, including the UK GDPR and Data Protection Act 2018, does not prevent the sharing of information for the purposes of keeping children safe and promoting their welfare. Where staff have a safeguarding concern, they must not assume that someone else will take action or share information.

Staff and volunteers will follow the principles below:

- The child's safety and welfare are the first consideration.
- Information will be shared promptly where this is necessary to safeguard or promote the welfare of a child.
- Information will be relevant, necessary, accurate, proportionate and shared securely.
- Information will only be shared with individuals or agencies who have a legitimate safeguarding role or need to know.
- Wherever it is safe and appropriate to do so, children and families will be informed about what information is being shared, with whom and why.
- Consent will not be treated as the default lawful basis for sharing safeguarding information. Information may be shared without consent where there is a safeguarding concern, where seeking consent may increase risk, or where another lawful basis applies.
- Decisions to share, or not to share, information will be recorded, including the reasons for the decision and who the information was shared with.
- Staff who are unsure whether to share information must seek advice from the DSL or deputy DSL without delay.

4. Breaking confidentiality

Confidentiality must be broken where this is necessary to safeguard a child, protect a child or another person from harm, prevent a crime, comply with legal duties, or support statutory safeguarding processes. In these circumstances, staff will share information with the DSL or deputy DSL and, where appropriate, children's social care, police, health services or other relevant agencies.

- 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.

5. Responsible use of ICT and technology

Staff must use school technology, online platforms and communication systems in a way that protects confidentiality, safeguards children and maintains professional boundaries. Communication with pupils and parents must take place only through approved school systems.

Staff must report concerns linked to online harm, harmful content, contact, conduct, commerce, cyber security, digitally manipulated images, AI-generated content or technology-facilitated abuse to the DSL or headteacher without delay.

The school will maintain appropriate filtering and monitoring arrangements in line with DfE expectations. Staff must not attempt to bypass filtering, monitoring or security systems and must report any weaknesses, concerns or incidents immediately. Filtering and monitoring arrangements will be reviewed at least annually by the responsible senior leader, with support from the DSL and IT support, and records of checks and actions will be maintained.

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 headteacher.

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 headteacher 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.

6. Management and security of school records

Safeguarding and child protection records will be kept securely, separate from the main pupil file where appropriate, and only accessible to those with a legitimate need to know. Records will be accurate, factual, timely and sufficiently detailed to support safeguarding decision-making.

When a pupil moves to another school or education provider, the DSL will ensure that relevant safeguarding information and the child protection file are transferred securely and promptly in line with statutory guidance and local safeguarding procedures. The school will retain evidence that the file has been transferred.

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

7. 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.

Staff, volunteers and governors remain bound by confidentiality expectations after leaving the school. They must not retain, copy, disclose or discuss confidential school information, including information about pupils, families, staff, safeguarding matters, governance or school operations, unless legally required to do so or authorised by the school.

The school will not share any information held on the departing staff member, unless there is an obligation to do so or consent has been obtained – 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 headteacher 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 by **their replacement**.

8. Monitoring and review

This policy will be monitored for effectiveness by the headteacher, DSL and DPO and reviewed annually, or sooner where there are changes to legislation, statutory guidance, DfE guidance, local safeguarding arrangements, data protection requirements, technology use, safeguarding risks or school procedures.

All changes will be communicated to relevant stakeholders.

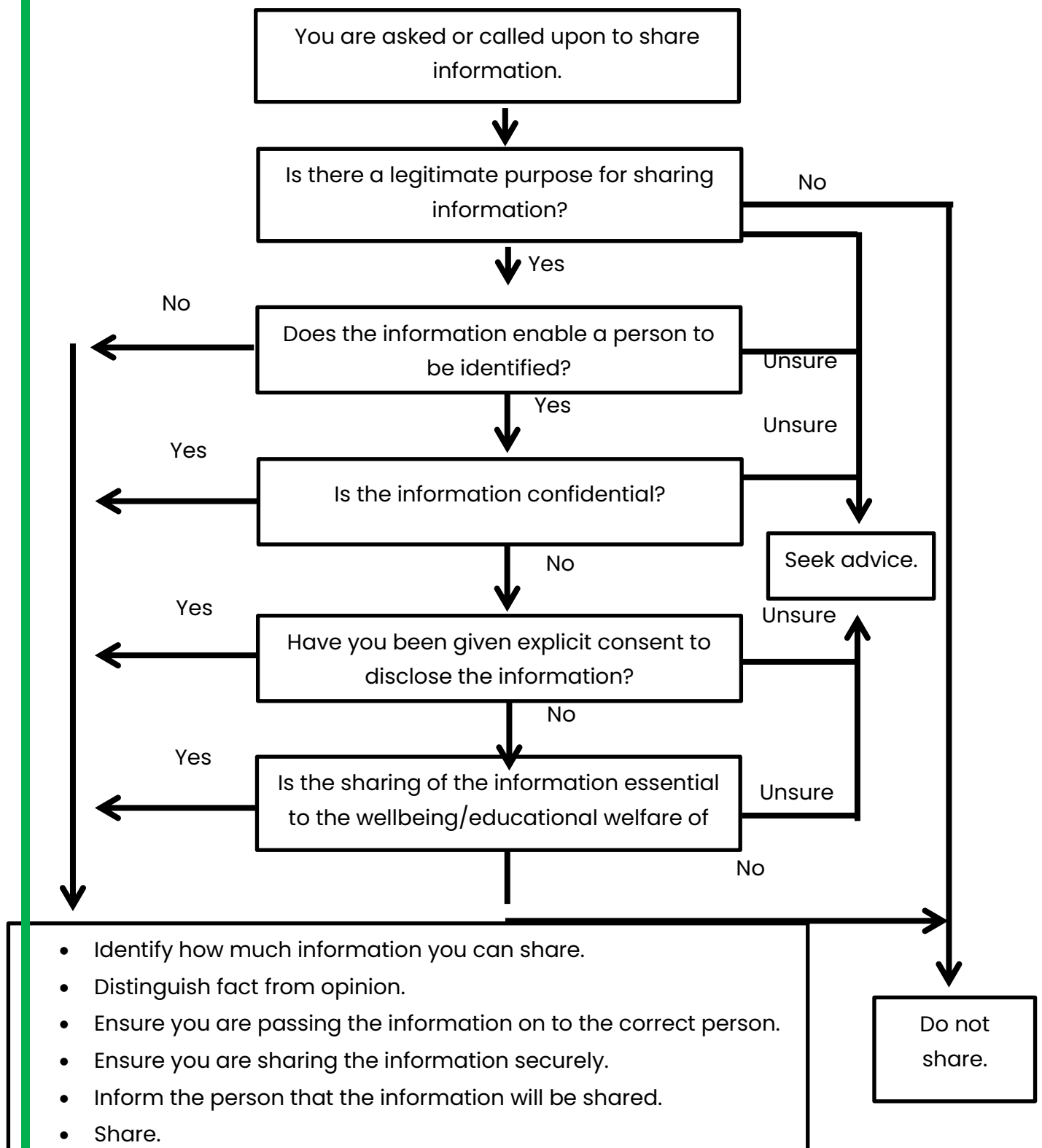
A record of information which has been shared will be continuously kept up-to-date.

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 in the school office and can be accessed by all appropriate staff members.

On an **annual** basis, the headteacher 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 headteacher acknowledges it in writing within <u>one week</u> .		
Begin the recruitment process, if appropriate.		
The <u>headteacher</u> informs the relevant staff, e.g. HR departments.		
The SBM 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.		
A handover period is established, if necessary.		

The Headteacher and DPO establish what information the school needs to keep pertaining to the departing staff member, who is informed of this.		
The SBM ensures the ICT technician terminates the departing staff member's accounts at the school and obtains any school-owned equipment.		
The School Business 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 Headteacher arranges for someone to fulfil any additional roles that the departing staff member has, e.g. fire safety officer or first aider.		
The Headteacher 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.		
Where the departing staff member had access to password protected sensitive data, e.g. bank accounts, the Headteacher or SLT member changes the passwords upon their departure.		

Where necessary, an information settlement agreement is established.		
--	--	--