




**Respect  
Collaboration  
of Schools**

## Confidentiality Policy

<b>Date approved</b>	March 2024	<b>Approved by</b>	Resources
<b>Review cycle</b>	2 years	<b>Signature</b>	
<b>Date for review</b>	March 2026	<b>Author</b>	Director of Operations

### Scope

This policy applies to all stakeholders in school and those who wish to be part of the schools community

### Principles

Respect Collaboration of Schools (The School) values the dignity of every individual member of staff and will apply this policy fairly and consistently in line with its core values of RESPECT. We will explore reasonable adjustments in applying this procedure to employees with a disability.

### 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
- The UK General Data Protection Regulation
- Data Protection Act 2018
- Education Act 2002
- Human Rights Act 1998
- The Education (Pupil Information) (England) (Amendment) Regulations 2019

This policy is compliant under the following case law:

- The Common Law Duty of Confidentiality

This policy also has due regard to guidance documents including, but not limited to, the following:

- DfE (2023) 'Keeping children safe in education'
- DfE (2018) 'Information sharing'
- DfE (2023) 'Working Together to Safeguard Children'

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

### Introduction and Context

This school recognises that a clear confidentiality policy will support the school in ensuring that young people are safe and healthy.

All staff seek to adopt an open and accepting attitude towards children and young people as part of their general responsibility for pastoral care.

Data will be processed in line with the requirements and protections set out in the UK General Data Protection Regulations.

### **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.

### **Roles and responsibilities**

**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 staff, pupils and parents, confidential.

The **Headteacher** 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 sign confidentiality agreements.
- 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.

### **Confidentiality and child protection**

The school will aim to strike a balance between confidentiality and trust, ensuring the safety, wellbeing and protection of our pupils.

The contents of this section operate in conjunction with the Allegations of Abuse Against Staff Policy.

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.

The school recognises that unfounded allegations do happen, and any 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 will not ordinarily be shared with any other staff, pupils or parents who are not involved in the investigation.

As an employer, the school has a duty of care for its employees; meaning that anyone who possesses relevant information and is involved in an investigation will not disclose any information beyond the individuals involved.

Anyone involved in the initial assessment of an allegation will attend an allegations management meeting and share all the relevant information they have about the person who is the subject of an allegation, and about the alleged victim.

Relevant information may include files or data stored on the alleged individual's school hard drive. The school will not carry out investigations on the alleged person's personal devices; this will be carried out by the police if necessary.

Where the police are involved, the school will ask the police to obtain consent from the individuals involved to share their statements and evidence for use in the school's disciplinary process. This will be done as the investigation proceeds to enable the police to share relevant information whilst avoiding any delay to the conclusion of the investigation or court case.

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/General Teaching Council for Wales 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 be contractually obliged to immediately inform the Headteacher 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.

### **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 withholds the right to take the appropriate civil, legal or disciplinary action. All non-teaching staff and volunteers will report safeguarding concerns to the DSL as soon as possible and in an appropriate setting.

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 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 individual responsible will be liable for disciplinary or legal action in accordance with the Data Protection Policy.

The DSL recognises and assures 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.

The school will ensure that all applicable staff have due regard to the relevant data protection principles, which allow them to share and withhold personal information. This includes:

- Being confident of the processing conditions which enable the storing and sharing of information for the purposes of safeguarding – such sensitive and personal information will be treated as 'special category personal data'.
- Understanding that the 'safeguarding of children and individuals at risk' is a condition allowing staff to share special category personal data – this includes sharing information without consent where the sharing of this information will enhance safeguarding or solve a safeguarding issue in a timely manner.
- Withholding the provision of data in compliance with the school's obligations under the Data Protection Act 2018 and the UK GDPR – where in doubt, the school will seek independent legal advice.

Where necessary, advice will be sought from the DPO and other practitioners to ensure all data is shared correctly.

Where possible, information will be shared with consent from the data subject, unless the school is able to proceed without consent under the UK GDPR and Data Protection Act 2018, e.g. if the data subject's safety is at risk.

Individuals' safety and wellbeing will form the base of all information sharing decisions, and information will not be shared if anyone's safety or wellbeing could be compromised.

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.

### **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.

### **Staff Confidentiality**

For employment related issues and processes Staff should refer to the Staff Code of Conduct (Section 8), Whistleblowing Policy (Section 8 and 9) and the Disciplinary and Dismissals Policy (Sections 4.8, 6.7 and Appendix 2). Staff should also be cognisant of other policies where there could be confidentiality breaches.

Staff breaches at any level of confidentiality could lead to an investigation, disciplinary action and, potentially, dismissal.

### **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 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.

### **Accessing information**

In accordance with article 15 of the UK GDPR, personal information, such as educational records, can be shared via a subject access request (SAR).

These requests must be made in writing to the Director of Operations and will be responded to within 15 school days if the request is regarding an educational record.

If the data being requested is not in relation to an educational record, the response must be within one calendar month.

Pupils, or the parent of a pupil, have the right to access the information that the school holds about the child in question.

Some types of personal data are exempt from the right of a SAR and so cannot be obtained by making a SAR. Information may be exempt because of its nature or because of the effect its disclosure is likely to have.

Information regarding another individual must not be disclosed in a SAR.

Individual requests for non-personal information cannot be treated as a SAR but will be managed as a Freedom of Information (Fol) request.

In line with the Freedom of Information Act 2000, private data and public records can potentially be accessed through lodging an Fol request.

Any request for information that appears to meet the criteria for a Freedom of Information disclosure will be directed to Derby City Council. Alternatively the request can be made directly to the council using the following link

<https://www.derby.gov.uk/council-and-democracy/open-data-freedom-of-information/freedom-of-information-environmental-information-regulations/#page-1>

Successful Fol requests will be responded to within 20 working days from receipt of the request, unless the request does not comply with the procedure set out in the school's Freedom of Information Policy.

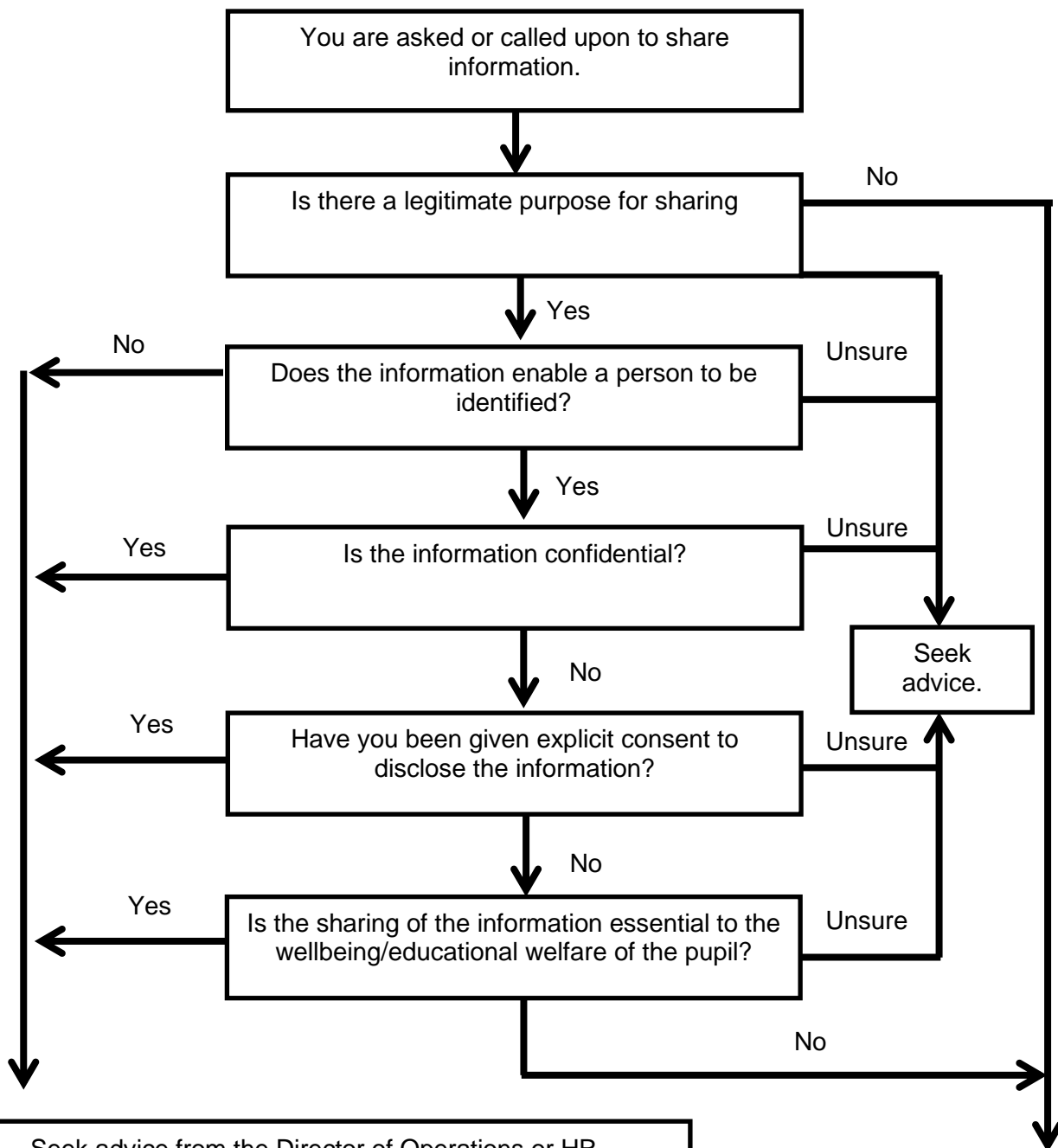
Certain information will not be shared, such as that explained in Part 2 of the Freedom of Information Act 2000.

### **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

## Appendix A – Information Sharing Flowchart



- Seek advice from the Director of Operations or HR Manager to identify how much information you can share.
- Distinguish fact from opinion.
- Ensure you are passing the information on to the correct person.
- Ensure you are sharing the information securely.

Do not share.

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





**Respect  
Collaboration  
of Schools**

# Confidentiality Statement

This is an agreement between The Respect collaboration of Schools and \_\_\_\_\_  
(external agency) dated \_\_\_\_\_.

This agreement outlines the need to ensure pupil and family confidentiality remains of the utmost importance and meets the expectations of the Data Protection Act 2018.

The School will handle any requests for access to personal data courteously, promptly and appropriately, making sure that either the data subject or authorised representative has the proper right to access under the 2018 Data Protection Act.

The School and any other agency accessing personal information on any of our learners will agree to:

- ❖ Acknowledge the rights of individuals to whom personal data relates and make sure that they can use these rights in accordance with the 2018 Act.
- ❖ Make sure that the collecting and using of personal data is carried out in a way that recognises the Fair Processing Code, which means that personal data is obtained fairly and lawfully.
- ❖ Only obtain and process personal data as specified in its notification.
- ❖ Collect and process personal data on a **need to know** basis making sure that it is accurate, not excessive and is disposed of at a time appropriate to its purpose.
- ❖ Make sure that for all personal data it takes the correct security measures – both technically and organisationally – to protect against loss, damage or misuse
- ❖ Make sure that the movement of personal data is carried out in a lawful way, both inside and outside of the School and that suitable safeguards are in place at all times.

## Confidentiality

During sensitive lessons and discussions, you may learn of personal information about a young person, it is important that you keep this information confidential except for the below reasons:

- where there is a child protection concern
- where there is risk of significant harm or threat to life
- where a pupil needs urgent medical treatment
- where potential or actual serious crime is involved
- where safeguarding national security is involved eg terrorism.

If you have concerns regarding a child, you will raise these in accordance with The Schools Safeguarding Policy and fulfil your duty to safeguard pupils at all times.

By signing this agreement, you are agreeing to the above terms and conditions.

Name: \_\_\_\_\_

Date: \_\_\_\_\_

Signature: \_\_\_\_\_

# Guidance on School Specific Information

## 1. Examples of where a confidentiality policy might be of use:

- A pupil knows someone who is bullying others at the school but is unsure about whether or not to tell.
- A pupil starts sharing something very personal in a classroom situation.
- A school uses staff or peers as a support system for pupils, e.g. listening, befriending.
- A pupil tells a member of staff that they are pregnant or sexually active.
- A pupil informs a lunchtime supervisor that their Dad is hitting their Mum.
- A pupil talks to a member of staff about their knowledge of a crime, e.g. shoplifting, assault.

## 2. Exceptions to Confidentiality

Likely exceptions requiring consideration by the school might include:

- where there is a child protection concern
- where there is risk of significant harm or threat to life
- where a pupil needs urgent medical treatment
- where potential or actual serious crime is involved
- where safeguarding national security is involved eg terrorism.

This must be consistent with other policies.

## 3. Age-related Considerations

Confidentiality issues need to take into consideration the differing abilities of pupils to understand the consequences of their choices. This understanding depends on the level of maturity of each individual, but there may be some correlation to their age.

The judge in the Victoria Gillick case gave the following general advice:

*"It is suggested that a child or young person's ability to make decisions about his/her life depends on him/her having "sufficient understanding and intelligence to be capable of making up his/her own mind".*

Before sharing any disclosed information with parents/carers, schools need to either obtain the consent of the pupil or consider the possible consequences of sharing the information, taking into account knowledge of family circumstances. This will need to be done on a case by case basis.

Each school will need to consider issues relating to confidentiality and the age/maturity of their pupils.