Confidentiality Policy

Sussex Road Primary School

Approved by:	HT	**Date:**	September 2026
Next review due:	September 2027		

Policy Statement

This confidentiality policy has been written to reflect the current guidance and legislation issued in relation to safeguarding children and promoting their welfare, whilst also taking into account data protection legislation. This includes, but is not limited to the principles of

- The Human Rights Act 1998,
- The Freedom of Information Act 2000,
- The Data Protection Act 2018
- Crime and Disorder Act 1998 S17,
- Children Act 1989 S17 and 47,
- Children Act 2004 S10, 11 and 12
- Section 40 of the Child Care Act 2006 welfare regulations

This policy should be accessed in conjunction with other school policies, including:-

- Acceptable Use Policy
- Allegations Against Staff Policy
- Anti-Bullying Policy
- Behaviour Procedure and Policy
- Data Management Policy and GDPR Guidance
- Staff Code of Conduct

The Senior Leadership Team are responsible for implementation, monitoring and review of this policy.

Definition of Confidentiality

For the purpose of this policy the following definition of confidentiality will apply: “discretion in keeping private information”.

In practice there are few situations where absolute confidentiality is offered by the school. We must strike a balance between ensuring the safety, well-being and protection of our pupils and staff, developing an ethos of trust where pupils, parents/carers and staff can ask for help when they need it and making sure that when it is essential to share personal information, good practice is followed.

In most cases we provide 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.

Rationale

As part of the ethos of our school, we take our responsibility to ensure the protection, health, safety and well-being of pupils entrusted to our care seriously. We expect all staff, including visitors and volunteers, to comply with this policy and will treat any breaches of confidentiality as a serious matter. Concerns will be managed in line with existing policies, including but not limited to our behaviour and complaints policy

We aim to ensure that all members of our community can share information in the confidence that it will only be used to enhance the education and welfare of children. At Sussex Road School we believe that:

- The safety, wellbeing and protection of children are of paramount consideration in all decisions about confidentiality. The appropriate sharing of information between staff is an essential element of ensuring the well-being of pupils in our care and any issues will be referred to the school Designated Safeguarding Lead (DSL) Team.
- This policy is implemented to ensure the number of situations when personal information is shared are minimised to enable our whole community to feel supported and safe to seek help both within and outside the school.
- Everyone in the school is made aware that no one can offer absolute confidentiality; our community needs to know the boundaries of confidentiality in order to feel safe and comfortable in discussing personal issues.
- The schools' approach and attitude to confidentiality is open and easily understood; everyone should be able to trust the boundaries of confidentiality operating within the school.

Key Guidelines and Principles

All information about individual pupils, their families and our staff, are private and will only be shared with those that need to know. In the case of confidential information relating to illegal activity, the school will take action in line with existing policies, including our child protection policy. The school will act in the best interests of children at all times whilst adhering to the law.

The school actively promotes a positive ethos and respect for the individual:

- All pupils have a right to the same level of confidentiality irrespective of gender, race, religion, medical concerns and special educational needs.
- There is clear guidance for the handling of child protection concerns and all staff have regular training on safeguarding and child protection.
- There is clear guidance for procedures to follow if a member of staff is accused of abuse or inappropriate conduct.
- Staff are aware of the need to handle all issues about different types of families in a sensitive manner.
- Any intolerance about gender, faith, race, culture or sexuality is unacceptable and will be responded to in line with the school's policies.
- Information collected for one purpose will not be used for another.

- Staff induction includes an awareness of the importance of confidentiality.

The school prides itself on good communication and staff are always available to talk to pupils and/or parents/carers about issues that are causing concern.

Parents/carers, pupils and staff need to be aware that the school has a duty to report and respond to child protection issues. When appropriate, staff will make clear that there are limits to confidentiality and parents/carers and pupils should feel reassured that only in exceptional circumstances will confidentiality be broken. An example of this is if a pupil asks if a member of staff can keep information secret.

Pupils will be informed when there is a need to tell someone else about a concern and they will be encouraged to do this for themselves when appropriate, for example, discussing an issue with a parent or carer. In some cases the school will support pupils to talk to their parent/carers within an agreed timescale, following advice from the DSL or Assistants DSLs as appropriate to the individual concern or circumstances.

The school will share any child protection concerns with parents/carers before going on to inform the correct authorities, unless by doing this a child or a parent could be placed in danger, or a criminal offence has taken place.

RHSE Lessons

Confidentiality is a whole school issue. Staff should be aware that effective relationship and sex education (RSHE) that brings an understanding of what is and is not acceptable behaviour may lead to pupils reporting child protection concerns. Staff will follow the Child Protection Policy if this occurs.

Clear ground rules will be set for RHSE Lessons and classroom work to reduce pupil and staff anxiety and minimise unconsidered, unintended personal disclosures. At the beginning of RSHE sessions, pupils will be reminded of the ground rules. Example of ground rules may include

- We won't ask each other or staff any personal questions.
- If we are worried about someone else's safety we will talk to a member of staff.
- We will listen to others views and opinion and will respect each other.
- If we find out things about other pupils/staff/parents which are personal and private, we won't talk about it, but if we are worried about someone's safety, we will tell a trusted adult.
- We can pass or opt out of something if it makes us feel uncomfortable.

The principles we follow in school are that in all cases where a pupil raises a concern, we:

- Ensure the time and place to speak about confidential issues are appropriate. When they are not, we reassure individuals that we understand they need to discuss something very important and that it warrants time, space and privacy

- See the pupil before the end of the school day. More serious concerns, for example where there is a potential child protection concern, will be reported immediately to the DSL or assistant DSLs to ensure that any necessary interventions to protect the pupil are accessed as early as possible
- Tell the pupil we cannot guarantee confidentiality if we think it will impact on theirs or someone else safety
- Do not interrogate pupils or ask leading questions that could jeopardise an investigation.
- Seek advice when there is a child protection concern, so that pupils are not put in the position of having to repeat distressing matters to several people.
- Encourage the pupil, whenever possible to confide in their parents/carers.

Information about pupils will be shared with parents, but only about their child. Parents will not be allowed access to other children's books, marks and progress grades. Parents should be aware that information about their child will be shared with the receiving school if/when they transfer. Addresses and telephone numbers of parents and pupils will not be passed on except in exceptional circumstances or to a receiving school.

All personal information about pupils will be regarded as confidential. Staff will be made aware of children with medical needs and class information will be accessible to staff who need that information, but not on general view to others. Information regarding health and SEND reports will only be shared as necessary and will kept securely. Logs of administration of medication will be kept secure and each pupil will have their own individual records. In all other notes, briefing sheets etc. pupils will not be identified.

Staff and Visitor Responsibilities

All staff (including non-teaching staff, student helpers and volunteers) and visitors, including professionals engaged in commissioned services on behalf of the school will

- Be made aware of this policy and the requirement to respect and follow it.
- Be reminded that the interest and welfare of the child is paramount.
- Required to abide by the School's Child Protection and Codes of Conduct at all times.
- Not discuss personal information given by parents with other members of staff except where it affects planning for a pupils needs.
- Inform pupils/parents/carers at the outset, that they cannot offer complete confidentiality in circumstances when they are concerns for a child, parents or staff members' safety and/or well-being.
- Explain to pupils/parent/carers openly and honestly what and how information will or could be shared and why and seek their agreement the exception being when to do so would place a child or others at risk of significant harm or if it would undermine the prevention, detection or prosecution of a serious crime.
- Inform any pupil/parent/carer/staff member that they may need to share safeguarding and/or well-being information with the DSL or Assistant DSLs if the concern relates to the behaviour of a member of staff.

- Ensure that the information they share is accurate, up to date, necessary for the purpose for which they are sharing it, shared only with those people who need to see it and shared securely.
- Unless they are already known, ensure any requests to share information from a professional are verified before information is divulged. This may include contacting the organisation they represent, for example police or Children's Social Care, directly rather than via a mobile phone number.
- Be duty bound to act appropriately upon information given to them directly as well as information not shared directly and consult with the school DSL or Assistant DSLs if they are unsure at any time.
- Seek advice, for example via the school data protection officer or the local authority, where there is doubt about the sharing of information.

Visitors and external contractors, for example health professionals, may have their own code of practice dealing with confidentiality. Where this is the case, the information that can and cannot be shared will be discussed and agreed.

Governors, staff, and volunteers need to be mindful that if they spend time in school, they may have access to information that is not general knowledge. It is essential that information, including things heard in a less formal manner, are not discussed outside of the school, as gossip of any kind is potentially damaging to all stakeholders.

Governors will be mindful that confidential issues about staff and pupils may be discussed or brought to their attention.

- General reports relating to individual pupils with SEN, Safeguarding Concerns and individual Staff TCP awards will be redacted when submitted to the Full Governing Board
- Confidential papers will be returned to the school to be destroyed appropriately.
- Governors will observe complete confidentiality when asked to do so by the governing body, especially in relation to matters concerning individual staff, pupils or parents.
- Although decisions reached at governors' meetings are normally made public through the minutes or otherwise, the discussions on which decisions are based will be regarded as confidential.
- Governors will exercise the highest degree of prudence when discussion of potentially contentious issues arises outside the governing body.

Staff may have support needs themselves in dealing with some of the personal issues of our pupils. We encourage staff to ask for help rather than possibly making poor decisions because they don't have all the facts and we do not want staff taking worries about pupils' home with them. There are many agencies we can refer pupils to if there is a need for additional support and we have procedures to ensure this happens. Working together as part of a team to support our pupils and asking for help is a way we ensure the school is a happy and safe learning environment.

The School's staff should discuss any concerns with their line manager, the DSL or assistant DSLs. Any unresolved issues will be respond to in line with school policies including our Child Protection, Complaints, Staff Code of Conduct, Allegations Against Staff and Whistleblowing policies.

Record Keeping and Access to Information

Records held in school, include:

Developmental/Educational Records

This includes observations of pupils, samples of their work, summary developmental reports and records of their achievements. These records are kept list as appropriate e.g. in a locked cupboard and can be accessed and contributed to by staff, pupils and their parents/carers.

Pupil's personal records

This includes registration and admission forms, medical information, signed consents and correspondence concerning the pupil or family, reports or minutes concerning the child from other agencies, observations by staff on any confidential matter involving the pupil, such as developmental concerns or child protection welfare/matters.
Personal and confidential records are stored as is appropriate e.g. in a lockable file or cabinet or secure/password protected/encrypted electronic system which cannot be accessed by individuals other than relevant staff.
Parents have access to the files and records of their own children in line with our Data Management Policy, but do not have access to information about any other child. Parents do not, however, have an automatic right of access to child protection records.

Other records

Issues to do with the employment of staff, whether paid or unpaid will remain confidential to the people directly involved with making personnel decisions.

The school acknowledges that:

Pupils and their parents/carers have a right to gain access to processed information upon written request.
Agencies such as the Police and Children's Social Work Services may gain a court order to access processed information, which the school deems confidential. This can also include the Local Authority's legal department and insurers, as well as other solicitors, for example in custody cases.

Any information recorded about a pupil will be written in a way that assumes it will be read by either the pupil or their parents/carers. Any processed information will be stored in accordance with Data Protection legislation and as outlined in our Data Management Policy and GDPR Procedures.

When confidentiality should be broken - procedures

The school recognises that all matters relating to child protection are confidential. The DSL will decide what information needs to be shared, with whom, how when and whether consent needs to be gained for this process. The DSL will share information about a pupil to other members of staff on a need to know basis only.

Members of the school community will be expected to follow our Child Protection Policy and Allegations Against Staff Policy where there are concerns about a pupil and/or member of staff.

If there are concerns and any member of the community is unsure of whether the information should be passed on or if other action should be taken, they should seek advice from the DSL, Assistant DSLs or the Local Authority. .If the DSL issues instructions that they should be kept informed of a concern, staff must comply. There is always a good reason for this, which staff may not know about.

Likely exceptions to confidentiality might include where:-

- there is a risk of harm or abuse, or where there is a threat to life.
- a pupil needs urgent medical treatment.
- a crime has been committed.
- safeguarding national security is involved e.g. terrorism.

Appendix A: Legislation

Human Rights Act 1998
Gives everyone the right to “respect for his private and family life, his home and his correspondence”, unless this is overridden by the “public interest”, e.g. for reasons of child protection, for the protection of public safety, public order, health or morals or for the rights and freedoms of others.

General Data Protection Regulations (GDPR) and Data Protection Act 2018
Applies to personal data of living, identifiable individuals, not anonymised data in manual and electronic records. Organisations who process personal data must comply with the data protection principles laid down in the Act.

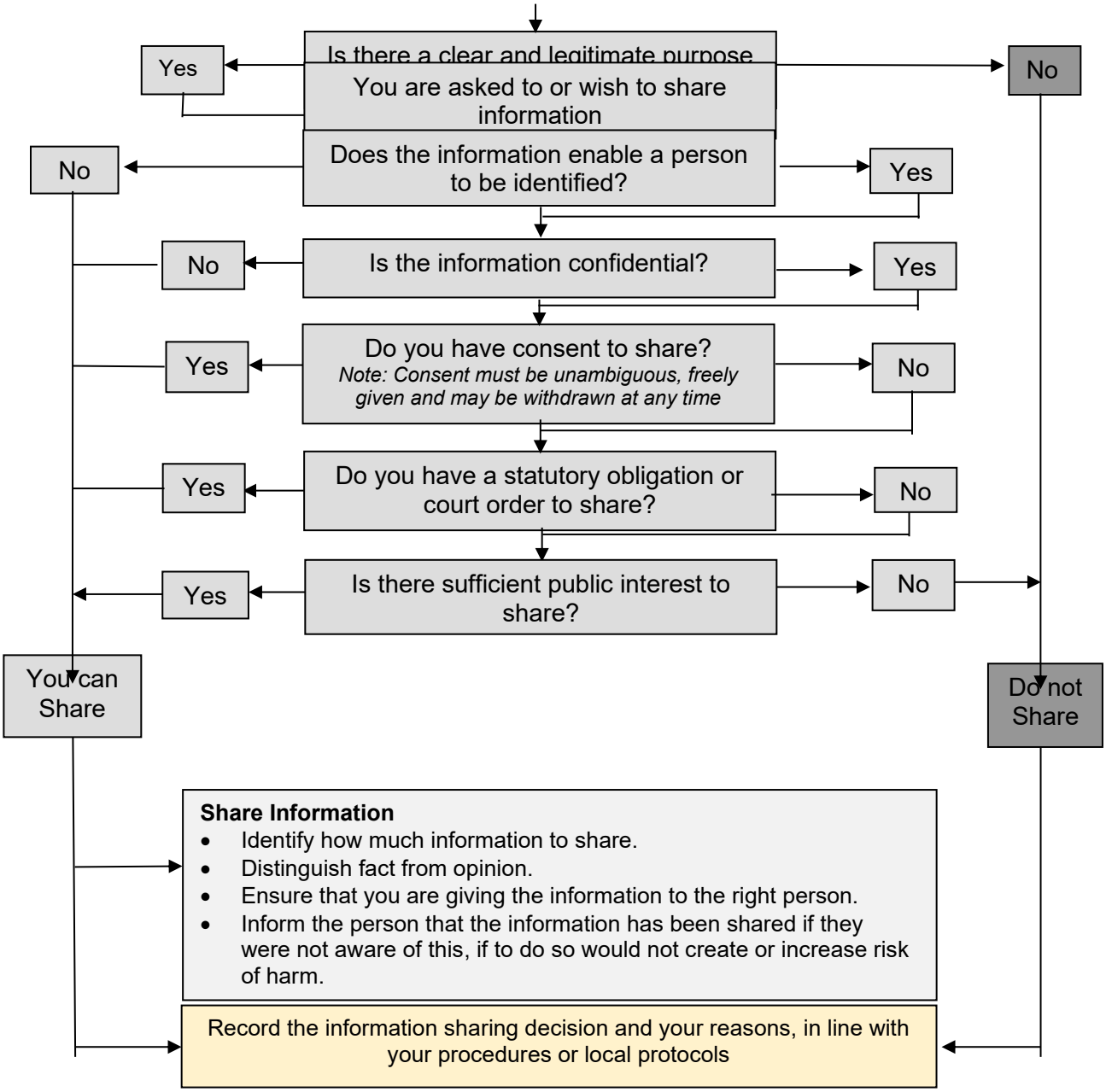
Schools need to be clear, when collecting personal data, what purposes it will be used for and should have policies to clarify this to staff, pupils and parents.

General Data Protection Regulation (GDPR), Data Protection Act 2018 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.

Freedom of Information Act 2000
Gives everyone the right to request any records from a public body, including settings, holds about them. A setting may withhold information it has if it is considered the information may damage the recipient, if disclosed. Settings data or record keeping policy should also cover the requirements of this Act.

Appendix B: Flowchart of Key Principles for Information Sharing

Adapted from 'Information sharing advice for safeguarding practitioners'



Seek advice from your line manager, Designated Safeguarding Lead, Data Protection Officer, and/or Local Authority if you are not sure what to do at any stage. Ensure that the outcome of the discussion is recorded.

Appendix C:

The Fraser Guidelines:

The case of Gillick v West Norfolk and Wisbeach Area Health Authority in 1985 settled the legal position for those working with children aged under 16 years old. During the Gillick case Lord Fraser stated that young people could receive advice or treatment without parental consent, but that key factors should be taken into account when assessing the young person's maturity to give consent. These are now referred to as the Fraser Guidelines:-

- The young person understands the advice being given.
- The young person cannot be convinced to involve parents/carers or allow the medical practitioner to do so on their behalf.
- It is likely that the young person will begin or continue having intercourse with or without treatment/contraception.
- Unless they receive treatment/contraception their physical or mental health (or both) is likely to suffer.
- The young person's best interests require contraceptive advice, treatment or supplies to be given without parental consent.

The 1985 Fraser guidelines identified doctors as key to this process, but it now accepted practice that the guidelines extend to other health care professionals.

The 6 Caldicott Principles

The Caldicott report was developed in 1977 and made recommendations relating to patient confidentiality. The Caldicott Report set out six key principles that health and social care organisations should use when reviewing its use of client information and the handling of client data.

Principle 1: Justify the purpose(s). Every proposed use of transfer of personally identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by the appropriate guardian.

Principle 2: Do not use personally identifiable information unless it is absolutely necessary. Where the use of personally identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing the ability to identify a person.

Principle 4: Access to personally identifiable information should be on a strict need to know basis. Only those individuals who need access to personally identifiable information should have access to it.

Principle 5: Everyone should be aware of their responsibilities. Action should be taken to ensure that those handling personally identifiable information are aware of their responsibilities and obligations to respect patient/client confidentiality.

Principle 6: Understand and comply with the law. Every use of personally identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.