

ST. PETER'S CHURCH OF ENGLAND PRIMARY SCHOOL



CONFIDENTIALITY AND INFORMATION SHARING POLICY

Date Written:

Revised December 2020 in line with KCSIE

Written by:

Richard Unthank- Head Teacher

Adopted by the LGB:

3rd December 2020

Date of Review:

September 2022

We have faith in our children

CONTENTS

SECTION 1	STATEMENT OF INTENT	Page 3
SECTION 2	ARRANGEMENTS	Page 4
2.1	Confidentiality	Page 4
2.2	Data Protection Act	Page 4
2.3	Freedom of Information Requests	Page 5
2.4	Information Sharing	Page 5
2.5	Legislation Guidelines	Page 7
2.6	Information held about Children	Page 8
2.7	Minutes of Governing Body Meetings	Page 8
2.8	Privacy Notices	Page 9
2.9	Transfer of Safeguarding Files	Page 9
2.10	Monitoring and Review	
SECTION 3	CONCLUSION	Page 11
Appendix A	Flowchart of when and how to share information	Page 12
Appendix B	Transfer of Child Protection Records (Template)	Page 13

SECTION 1

STATEMENT OF INTENT

St. Peter's Church of England Primary School recognises and accepts the responsibilities and duties which it has for confidentiality and data protection for all members of the school community.

However, the Governors and the Headteacher also recognise that information sharing is vital to safeguarding and promoting the welfare of children and young people.

The 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 pupil interest, for reasons of child protection, for the protection of public safety, pupil order, health or morals or for the rights and freedoms of others.

This policy aims to provide clear guidelines to all members of the school community, including staff, governors and volunteers, with regard to confidentiality and information sharing. It also aims to make explicit the school's commitment to the development of good practice and sound procedures to keep children and adults safe in our school. This is inclusive of the expectations from the Data Protection Act 2018 and General Data Protection Regulations 2018.

SECTION 2

ARRANGEMENTS

2.1 CONFIDENTIALITY

All adults are expected to maintain confidentiality and should adhere to the following principals:

- Appreciate the privileged environment of which they are a part and ensure that confidentiality is not breached
- Implement the school's Child Protection and Safeguarding Policies
- Maintain professional standards of confidentiality about anything seen or heard within the school
- Adhere to and enforce the school's procedures for the taking of and use of photographs and video recording in school
- No child's personal details will be given out over the telephone until the validity of the request has been ascertained via a returned call
- Unconditional confidentiality should never be given
- No adult should discuss an individual child's behaviour in the presence of another child
- No adult should enter into detailed discussion about a child's behaviour or academic progress with other children or their parents
- All adults adhere to all school policies and procedures with regards to e-safety, use of computers and social networking
- Confidential and/or sensitive information will only be discussed between staff on a "need to know" basis

2.2 DATA PROTECTION ACT

The [Data Protection Act](#) controls how your personal information is used by organisations, businesses or the government.

Everyone responsible for using data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the [European Economic Area](#) without adequate protection

There is stronger legal protection for more sensitive information, such as:

- ethnic background
- political opinions
- religious beliefs
- health
- sexual health
- criminal records

As an academy we follow the Galileo MAT Data Protection Policy. All data processors within school are mindful of the basic principles of data protection outlined in the policy and work within those boundaries.

2.3 **FREEDOM OF INFORMATION REQUESTS**

School will respond to any Freedom of Information requests within the permitted timescale. If in doubt as to the validity of any requests advice will be sought from Galileo MAT.

2.4 **INFORMATION SHARING**

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. Poor or non-existent information sharing is a factor repeatedly flagged up as an issue in Serious Case Reviews carried out following the death of, or serious injury to, a child.

As a school we adhere to the Government's seven golden rules when sharing information with other professionals:

1. Remember that the Data Protection Act 1998 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.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Share with informed consent where appropriate and, where possible, respect the wishes of those who do not consent to share confidential information. You may still share information without consent if, in your judgement, there is good reason to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case.

When you are sharing or requesting personal information from someone, be certain of the basis upon which you are doing so. Where you have consent, be mindful that an individual might not expect information to be shared.

5. **Consider safety and well-being:** Base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. **Necessary, proportionate, relevant, adequate, accurate, timely and secure:** Ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. **Keep a record of your decision and the reasons for it – whether it is to share information or not.** If you decide to share, then record what you have shared, with whom and for what purpose.

The Information Commissioner's Office (ico.) also provide a checklist which should be followed when deciding what, if any, data should be shared:

Is the sharing justified?

Key points to consider:

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and/or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider:

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share (for example was it given in confidence?).
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues:

- What information needs to be shared.
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it.
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

When and how to share information

The flowchart at Appendix B should be used when considering sharing information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- What information was shared and for what purpose.
- Who it was shared with.
- When it was shared.
- Your justification for sharing.
- Whether the information was shared with or without consent.

2.5 LEGISLATION GUIDELINES

The Education Act 2002, section 175 (for maintained schools and settings), the Education (Independent School Standards) Regulation 2014 (for Academies/Free Schools) and the Education non maintained Special schools (England) Regulation 2015 sets out the need for all schools/settings to have appropriate safeguarding arrangements in place.

The legislation also sets out the duty to work co-operatively with external organisations. Although the legislation for Data Protection and Human Rights is in place, the learning from serious case reviews is clear, ‘Where there are concerns about the safety of a child, the sharing of information in a timely and effective manner between organisations can reduce the risk of harm’ (Information Sharing, 2015) and therefore both internal and external procedures should always be in place for sharing information.

Section 10 and 14B of the Children Act 2004, is explicit in highlighting the need for all agencies to share information with each other, the Local Authority and the Local Safeguarding Children Partnerships.

The General Data Protection Regulations, 2018 states that if you are creating records about the children and/or adults that take part in your services or activities, you need to make sure they understand what records you hold, why you need to hold them and who you might share their information with (for example as part of a multi-agency child protection team) (Information Commissioner's Office, 2017(a) and 2017(b)). If you are keeping records for child protection reasons, you don't always need to gain consent from the adults and/or children concerned. Therefore information may still be held and retained as long as there is an agreed purpose for it and where applicable, consent has been given.

2.6 INFORMATION HELD ABOUT CHILDREN

- Information about children will be shared with parents/carers but only about their own child.
- Parents/carers will not have access to any other child's marks and progress grades at any time. However, parents/carers should be aware that information about their child will be shared with the receiving school, if and when they change school
- All personal information about children, including Social Care records are regarded as confidential. The Designated Safeguarding Lead (DSL) will decide who will have access, and whether those concerned have access to all, or only selected information
- Information regarding health reports such as speech therapy, medical reports, SEN reports, SEN minutes of meetings, Social Care and Health Services will be kept securely
- When a child leaving St. Peter's is admitted by another school the pupil records, excluding any SEN or safeguarding issues, will be sent electronically as a CTF file via the School to School system.

2.7 MINUTES OF GOVERNING BODY MEETINGS

- Governors, in particular those sitting on discipline committees, will not divulge details about individuals (be they staff, families or individual children) to any person outside of the meeting
- Governors need to be mindful that from time to time issues are discussed or brought to their attention about staff and children
- Governors must observe complete confidentiality when asked to do so by the governing body, especially in relation to matters concerning individual staff, children or parents/carers
- Although decisions reached at governors' meetings are normally made public through the minutes or otherwise, with the exception of Pay Review, the discussions on which decisions are based should be confidential

2.8 PRIVACY NOTICES

As an academy staff and pupil data is shared with the MAT and LA through the termly/annual census returns. Galileo Multi Academy Trust Privacy Notices are published and issued to outline why and how this information is required and used.

2.9 TRANSFER OF SAFEGUARDING FILES

When children transfer from one educational establishment to another, either at normal transfer stage or as the result of a move and records of child protection/welfare concerns exist, these should be sent to the receiving school as soon as possible, **preferably within 5 days.**

- Transfer should be arranged separately from the main pupil file in line with DfE Guidance in 'Keeping Children Safe in Education' (September 2020).
- Where children are dual registered (e.g. on roll at a mainstream school, but receiving education in another establishment, such as an Intervention Unit or Base), any existing child protection records should be shared with the new establishment **prior to the child starting**, to enable the new establishment to risk assess appropriately.
- In order to safeguard children effectively, it is important that when a child moves to a new educational establishment, the receiving establishment is immediately made aware of any **current** child protection concerns, preferably by telephone prior to the transfer of records.

Child Protection records must always be passed directly and securely to the Designated Safeguarding Lead in the receiving establishment.

- It is important that all child protection records are transferred at each stage of a child's education, up until the age of 18, or in some cases, beyond.

The responsibility for transfer of records lies with the originating setting, as the receiving setting might not otherwise know that child protection concerns exist. The onus is therefore on the originating setting to facilitate the secure transfer of records, not on the receiving setting to make contact and collect the records.

Paper or electronic records containing child protection information must be transferred in the most secure method available to the establishment:


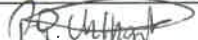
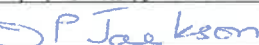
- By hand if possible.
- If paper records are posted this should be by 'signed-for' delivery;
- Electronic records must only be transferred by a **secure** electronic

- transfer mechanism or after the information has been encrypted.
- Any receiving schools using CPOMS can be sent our electronic records if requested

Whether CP files are passed on by hand, by post or electronically, written evidence of this transfer (e.g. the form at Appendix B of this document) appropriately signed and dated, should be retained by both the originating and receiving setting. It is recommended that the originating establishment keeps a **copy of the form** along with a copy of the chronology of events and any records pertaining to the establishment in line with retention guidance.

2.10 MONITORING AND REVIEW

The Dedicated Safeguarding Lead, the Headteacher and the Dedicated Safeguarding Governor will monitor this policy throughout the year and update as and when necessary.

Name	Title	Signature	Date
Susan Hunt	Assistant Headteacher / DSL		03/12/20
Richard Unthank	Headteacher / DDSL		03/12/20
David Jackson	Chair of Local Governing Body		03/12/20

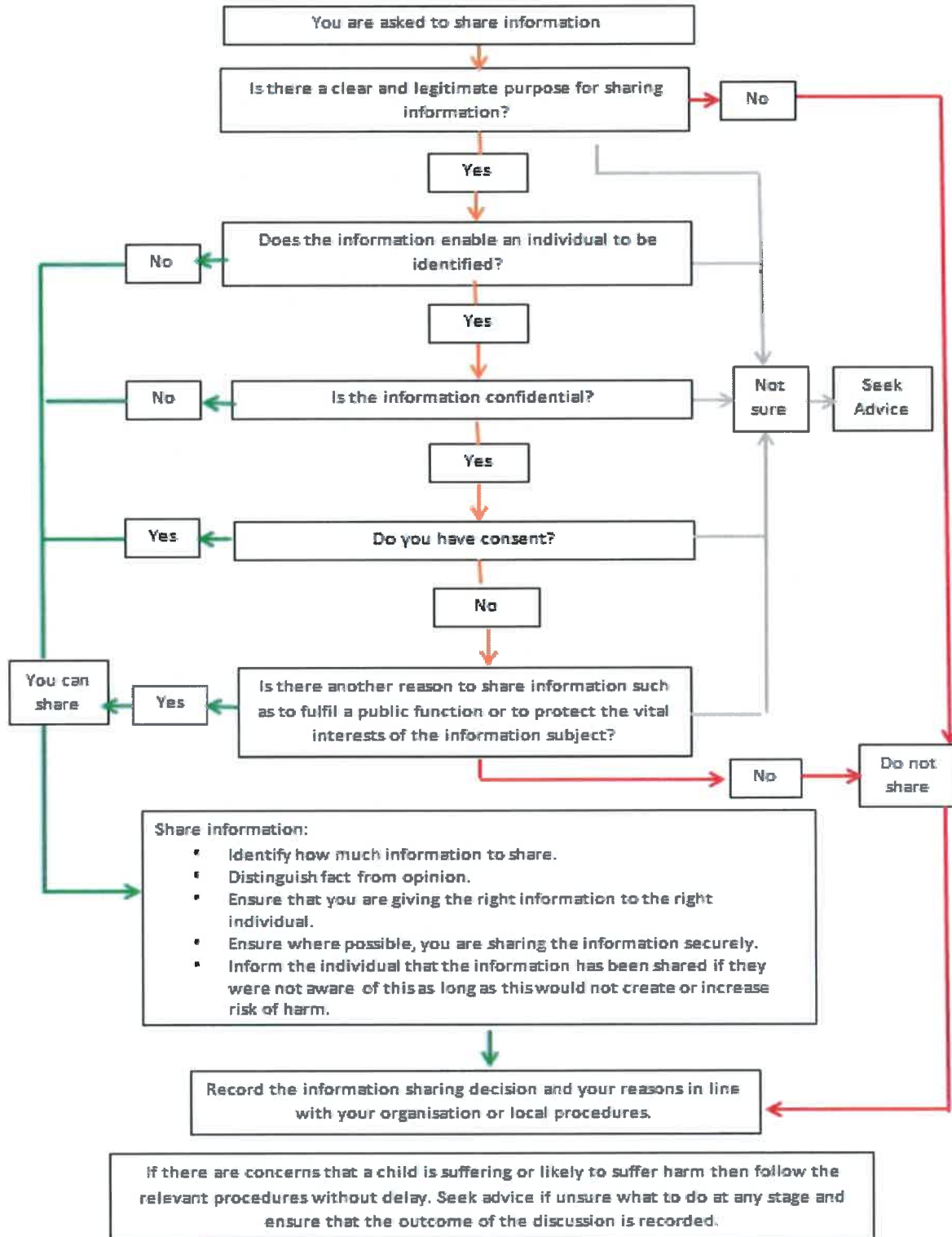
SECTION 3

CONCLUSION

Information regarding children who are vulnerable and their families will have to be recorded and stored in the best interests of those individuals. Where possible and at every opportunity children and adults should be informed of this and their consent gained and recorded alongside their consent to share this information with others. In some circumstances e.g. child protection, consent may not be given but the statutory nature of the case requires that it is recorded. In all circumstances, information should be treated confidentially, recorded factually and accurately and stored for an agreed period of time (see retention schedule). Parents and children have a right to know and understand what information is recorded about them and why and may request to see it. Any information that is shared must be appropriately redacted and pertain only to those individuals of whom the request has been made.

APPENDIX A

FLOWCHART OF WHEN AND HOW TO SHARE INFORMATION





St. Peter's Church of England Primary School
Marshall Drive
Brotton
SALTBURN-BY-THE-SEA
TS12 2UW

E-mail: office@stpetersceprimary.co.uk
Tel: 01287 676210
Fax: 01287 203023

TRANSFER OF SAFEGUARDING RECORDS

Name of Child:
Date of Birth: UPN:
Home address:
.....

Name of Designated Safeguarding Lead: Miss S. Hunt

Date file exchanged by hand: OR

Date file posted by recorded delivery: OR

Date information sent electronically:

Name of receiving establishment:

Address of receiving establishment:
.....

Name of receiving Designated Safeguarding Lead:

Date file received by hand: OR

Date file received by recorded delivery: OR

Date information received electronically:

Signature of Designated Safeguarding Lead:

Date:

Upon receipt, the receiving setting should:

- Sign this form and keep a copy with the child's CP records
- Ensure the original form is returned promptly to St. Peter's Church of England Primary School by either E-mail, fax or post

