Ravenswood School
Data Protection and Information Sharing Guidance Policy

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 2018, common law duty of confidentiality, current Information Sharing Guidance and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing and disclosure of personal data need to be aware of their duties and responsibilities by adhering to these guidelines.

Introduction

In order to enable us to provide education and other associated functions, Ravenswood School collects and uses personal information about staff, pupils, parents and other individuals who come into contact with the school. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

Ravenswood School, as a Data Controller, is registered with the Information Commissioner's Office (ICO) and details the information it holds and uses. We issue a Fair Processing Notice to all pupils/parents, which summarises the information held on pupils, why it is held and the other parties to whom it may be passed. We do everything possible to ensure the safety and security of any material of a personal or sensitive nature.

We issue a Fair Processing Notice to all staff and volunteers.

It is the responsibility of all members of the school community to take care when handling, using or transferring personal data to ensure it cannot be accessed by anyone who does not:

- have permission to access that data
- need to have access to that data.

Any loss or misuse of personal data can have serious consequences for both individuals and / or institutions. It can bring the school into disrepute and may well result in disciplinary action, fines or criminal prosecution. Therefore, anyone who has access to personal data must understand and adhere to this policy.

The Data Protection Act (2018) lays down a set of rules for processing of personal data (both structured manual records and digital records). It provides individuals with rights of access and security and requires users of data (data processors) to be open about how it is used and to follow "good information handling principles**".** Please see Appendix 1 for Subject Access Request Procedures.

Data Protection Officer

The Data Protection Officers role is to support the school to oversee and enforce compliance. They are there to guide staff and ensure we are doing all the right things to comply. The DPO carries no liability for any data handling issues or breaches.

Ravenswood is compliant with Data Protection Regulations and must be able to demonstrate this. This is proven using an internal audit system managed by the DPO. It is also the DPO's role to inform and educate staff on the importance of data protection within the school.

Personal Information

The school has access to a wide range of personal information and data; held in different formats such as digital or paper records.

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held. This will include:

- Personal information about members of the school community e.g. names, addresses, contact details, legal guardianship, health records, disciplinary records
- Academic data e.g. pupil progress records, Annual Reviews, End of Year Reports, college application forms
- Professional records eg application forms, employment history, taxation and national insurance records, appraisal records, health forms and references
- Any other information that might be disclosed by parents / carers or by other agencies working with families or staff members and shared in circumstances where the person giving the information could reasonably expect that it would not be shared with others.
- Information that is not already lawfully in the public domain

Sensitive Personal Information

Sensitive personal information consists of information relating to the racial or ethnic origin of a data subject, their political opinions, religious beliefs, trade union membership, sexual life, physical or mental health or condition, or criminal offences or record.

Where the school intends to process sensitive personal data, there are further conditions. If none of the following conditions can be met, processing cannot legally continue;

- where the data subject has given his explicit consent;
- where the processing is required for the purposes of complying with employment law;
- where it is necessary to establish, exercise or defend legal rights.

Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for one or more specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;

8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

General Statement

The school is committed to maintaining the above principles at all times. Therefore the school will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft, unauthorised disclosure or inappropriate disposal, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure our staff are aware of and understand our policies and procedures and their responsibility in handling personal information in a safe and secure manner.
- Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Secure storage of data and data access

All personal information must be stored in an appropriately well organised, secure and safe environment that avoids inappropriate access by unauthorised people, loss or electronic degradation.

The school ensures that paperwork and electronic files and folders are set up with appropriate permissions so that users can only access the data required by their role.

Classification	Examples	Who can access	Disposal
Unclassified	Information on the school website School Policies Names and photos of governors Terms of Office of governors Attendance of governors at meetings Pecuniary Interests of governors Governors' minutes Exam Results Names of staff & volunteers Displays of work Staff minutes Teaching strategies	The public	
Official Information	Names of pupils Photos of pupils Pupils work Sensitive information about pupils' health and social circumstances which is needed to keep a child safe and promote their wellbeing on a	All school staff Volunteers in classrooms Pupils and their families	Shred

	daily basis. All school staff governors used to support pupils, including parents and families Photos of staff and volunteers		
Official Sensitive - staff	Addresses and telephone numbers of staff Dates of birth of staff Employment history and contractual information National Insurance information Medical conditions Accidents at work	Admin team Interview panels Supply Cover Supervisor Senior Leadership Team	Shred
Official Sensitive - pupils	Addresses and telephone numbers of pupils Dates of birth of pupils Pupils Assessment Levels Sensitive information relating to pupils which is needed by those working routinely with the child to keep them safe and promote their wellbeing., eg Care Plans/Provision Maps/CHPs/Risk Assessments	Designated classteam Teachers Admin team Senior Leadership Team Childrens' Services Team	Shred
Confidential information - staff	Sensitive Personal information.	Senior Leadership team. Human Resources Occupational Health	
Confidential information - pupils	Sensitive Personal information relating to pupils and their families, which does not generally need to be shared.	Designated Safeguarding Lead and Deputy Designated Teacher for Looked After Children and Deputy	

ICT systems will enforce password complexity appropriate to the level of data security required; staff have strong passwords whilst pupils can use weaker ones. Password security is implemented in accordance with the school's E-Safety Policy.

Personal data may only be accessed through school systems which are securely password protected.

Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used.

If private equipment; i.e. owned by the users, is used to access storage of Official Sensitive data, it is the responsibility of the member of staff to ensure that any private equipment (computer, mobile devices) used to open school emails and attachments is password protected and does not retain the information on the hard drive.

Disposal of data

The school will comply with the requirements for the safe disposal of personal data when it is no longer required.

The disposal of electronic data deemed protected or higher, will be conducted in a way that makes reconstruction highly unlikely by securely wiping hard discs on computers, ipads and network servers and pen drives and CDs and DVDs.

Paper copies of data deemed official sensitive or confidential is shredded.

All disposal of hardware is organised by the Network Manager through a certified GDPR compliant company as listed on the GDPRIS supplier database.

Secure transfer of data and access out of school

The school recognises that personal data may be accessed by users out of school, or transferred to the LA or other multi-agency organisations. In these circumstances:

- Users may not remove or copy Official or Sensitive data from the school or authorised premises without permission from the Senior Leadership Team and unless the media is encrypted and password protected and is transported securely for storage in a secure location. Hard copies of Restricted data must be signed out and signed back in return.

- Encrypted email such as Egress Switch will be used with school email accounts when personal data needs to be shared electronically with other organisations.

- CONFIDENTIAL information may only be removed with agreement from the Headteacher. Hard copies of confidential data must be signed out and signed back in on return.

- Users must take particular care that computers or portable devices which contain personal data are not accessed by other users (e.g. family members) in or out of school.

- When personal data is required from outside the school's premises; e.g. by a member of staff working at home, they must use the school's official secure remote access system and school laptop.

- If secure remote access is not possible, users must only remove or copy personal or sensitive data from the school if the storage media is school or Council-issued, encrypted and is transported securely for storage in a secure location.

Audit Logging / Reporting / Incident Handling

Reporting a Data Protection Breach

When reporting a breach we first need to ask two questions:

1) Did it impact on anyone?
2) Was any harm done?

If the answer is yes to either of the above questions a breach must be reported within 72 hours. Using the GDPR is system we are able to manage the breach appropriately within the school. If the answer was no we can still choose to report it, treating it as a near miss. If we deem it necessary we will escalate the breach to the ICO (Information Commissioners Office) for further investigation.

The activities of data users, in respect of electronically held personal information, will be electronically logged. The audit logs will be kept by the Network Manager to provide evidence of accidental or deliberate security breaches, for example; loss of protected data or breaches of an acceptable usage policy.

The Network Manager will maintain an inventory of, and will audit all school ICT equipment such as desktop and laptop computers and all portable devices eg iPads and cameras.

Members of staff who are leaving must return all personally-issued ICT equipment to the Headteacher. Staff who are leaving will be required to sign a declaration confirming they have returned all school equipment and property, that they will not attempt to access school information after their leaving date.

Disclosure of educational records

Schools, as independent public bodies, are directly responsible under the Data Protection Act 1998 (DPA) for the collation, retention, storage and security of all information they produce and hold. This will include educational records, head teacher's reports and any other personal information of individuals; pupils, staff and parents.

The Pupil Information Regulations require that a school's governing body ensures that a pupil's educational record is made available for their parent to see, free of charge, within 15 school days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this too must be provided and within 15 school days.

Information Risk Incidents

All possible breaches of data protection must be reported immediately to the Headteacher, who will follow appropriate procedures. If the breach has not been contained the Headteacher will report it to North Somerset Council and work in conjunction with the Council to devise a plan of action for rapid resolution. A plan of action to prevent recurrence will also be developed.

Complaints

Complaints will be dealt with in accordance with the school's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator). Further advice and information is available from the Information Commissioner's Office, www.ico.org.uk or telephone 0303 1231113

ICT Service Continuity Management

The school has an ICT Service Continuity Plan (see the E-Safety Policy) that provides the framework for the school to develop a plan that considers the preparation for, response to and recovery from a disaster affecting all (or part) of the range of critical data held in the school's management information systems.

Information Sharing

Information Sharing is a key element of data protection safeguarding children and young people. Ravenswood School will explain to students and their families and staff what and how information will or could be shared, with whom and why and also seek their agreement when required.

It is the class teacher's responsibility to share confidential information appropriately, with their whole class team both permanent and temporary. This is to ensure children's care, safety and well-being, so must be the overriding consideration in making any decisions.

Any decision to share, or not share, information must be recorded, detailing the reason for the decision, what information has been shared, with whom and for what purpose.

If official Sensitive confidential information is shared, this must be in a professional manner to ensure compliance with current Information Sharing Policy and protocols.

Information sharing around Safeguarding Concerns:
Whilst parents have a right to expect that personal information they share with Ravenswood School will be regarded as confidential there are, however, certain circumstances when information can be shared without parents' consent, such as when;

- there is evidence that the child is suffering, or is at risk of suffering, significant harm
- there is reasonable cause to believe that a child may be suffering, or is at risk of suffering significant harm
- failing to share the information would put a pupil at increased risk of significant harm
- it would undermine the prevention, detection or prosecution of a serious crime

When sharing information without consent, Ravenswood School will always consider the safety and welfare of a student in making the decision. When there is a concern that a student may be suffering, or is at risk of suffering, significant harm, the student's safety and welfare will always be the overriding consideration. It is

the responsibility of the Safeguarding Lead or Deputy Safeguarding Lead to decide and provide authorisation to staff seeking to make a disclosure. Please see Appendix 2.

If information is shared, this will be recorded in the student safeguarding file in the following way:
What information was provided and to whom, the reason for sharing information and the name of the Safeguarding Lead disclosing the information together with the member of the Senior Leadership Team who authorised disclosure of information.

The Fraser ruling or Gillick case of competency will be considered for all children over 12 years of age to give their own consent to information being shared, as a child or young person with learning difficulties or disabilities maybe considered competent to make decisions. This is applied when a young person achieves sufficient understanding to understand and retain advice or information, sufficient maturity to understand what is involved and the implications remaining consistent in their view.

Key criteria to consider are;

- Can the young person understand the question being asked, having used appropriate age and ability related language or method of communication?

- Does the young person have a reasonable understanding of
  - What information might be recorded/shared?
  - The reasons why this happened?
  - The implications of information being recorded and shared?
- Can the young person
  - Appreciate and consider alternative courses of action?
  - Consider different aspects of a situation?
  - Express a clear personal view, as distinct from repeating what someone else thinks they should do?
  - Be reasonably consistent in their view on the matter?

This does not affect the parental right under the Educational Records Act to see their child's education records, until a child reaches the age of 16. Safeguarding guidance indicates that any sexual activity under the age of 16 is documented, including any decision not to share information. Whilst maintaining confidentiality with a student being worked with, Ravenswood School will encourage the student to share the information being discussed with their parents/carers if this is felt to be appropriate. Please see Appendix 1.

Appendix 1 – Guidance on Information Sharing Requests

Rights of access to information

There are three distinct rights of access to information held by schools;

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them. This right is commonly referred to as subject access requests (SARs), is created by Section 7 of the Data Protection Act. It can be used by individuals who want to see a copy of the information the school holds about them. They can request to be;

- given a description of the personal data, the reasons it is being processed, and whether it will be given to any other organisations or people;
- given a copy of the information comprising the data; and
- given details of the source of the data (where this is available).

2. The right of those entitled to have access to curricular and educational records as defined within the Education Records Regulations 2005 and 2008. The Pupil Information Regulations require that a school's governing body ensures that a pupil's educational record is made available for their parent to see, free of charge, within 15 school days of receipt of the parent's written request. If a parent makes a written request for a copy of the record this too must be provided and within 15 school days.
The procedures to follow are the same as for Subject Access Requests, however the time scales and fees differ. The Ravenswood Governing body may charge a fee for the copy but if they do, it must not be more than the cost of supply – see section 4.

3. A Freedom of Information request can be initiated by any person. The information disclosed through an FOI request will usually become public information, available to anyone. The response cannot, therefore include personal or sensitive information, as these are exempt from FOI requests. This may be subject to a fee, to be determined, on a case by case basis by the governing body.

Actioning a Subject Access Request, Pupil Information or Freedom of Information Request

1. Requests for information must be made in writing; which includes email, and be addressed to the Head teacher**.** If the initial request does not clearly identify the information required, then further enquiries will be made.
2. The identity of the requestor must be established before the disclosure of any personal or sensitive information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of at least two of the following, to establish identity and current address :

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Head teacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records to be disclosed. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The school may make a charge for the provision of information, dependent upon the following:
   - Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.
   - Of the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Head teacher.
   - Should the information requested be personal information that does not include any information contained within educational records the school can charge up to £10 to provide it.

5. The response time for Subject Access Requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees, identification and clarification of information sought

6. The response time for Pupil Information requests, once officially received, is 15 days (not working or school days but calendar days, irrespective of school holiday periods). However the 15 days will not commence until after receipt of identification and clarification of information sought, if required.

7. The response time for Freedom of Information requests, once officially received, is 15 days (not working or school days but calendar days, irrespective of school holiday periods). However the 15 days will not commence until after receipt of fees and clarification of information sought

8. The Data Protection Act 1998 allows exemptions as to the provision of some information; therefore all information will be reviewed prior to disclosure by the Head teacher.

9. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale for SARs.

10. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

11. If there are concerns over the disclosure of information then additional advice should be sought.

12. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

13. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

14. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Issue	Author/Owner	Date Reviewed	Approved by Governors on	Comments
1.	Business Committee	November 2016	23/11/16	
2.	Business Committee	November 2017	23/11/17	Updated ICO contact details. Updated in line with GDPR ready for May 2018
3	Business Committee	November 2018	19/12/18	Update to disposal of ICT equipment. Update to Secure Transfer of Data: using encrypted email Role of DPO updated

Appendix 2
Seven Golden rules for sharing information:

1. Remember that the 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.

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, or your information governance lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.

4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and Data Protection Act 2018 you may share information without consent if, in your judgement, there is a lawful basis 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 clear of the basis upon which you are doing so. Where you do not 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 General Data Protection Regulation (GDPR) and Data Protection Act 2018

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 introduce new elements to the data protection regime, superseding the Data Protection Act 1998. Practitioners must have due regard to the relevant data protection principles which allow them to share personal information,
The GDPR and Data Protection Act 2018 place greater significance on organisations being transparent and accountable in relation to their use of data. All organisations handling personal data need to have comprehensive and proportionate arrangements for collecting, storing, and sharing information.

The GDPR and Data Protection Act 2018 do not prevent, or limit, the sharing of information for the purposes of keeping children and young people safe.
To effectively share information:

• all practitioners should be confident of the processing conditions, which allow them to store, and share, the information that they need to carry out their safeguarding role. Information which is relevant to safeguarding will often be data which is considered 'special category personal data' meaning it is sensitive and personal

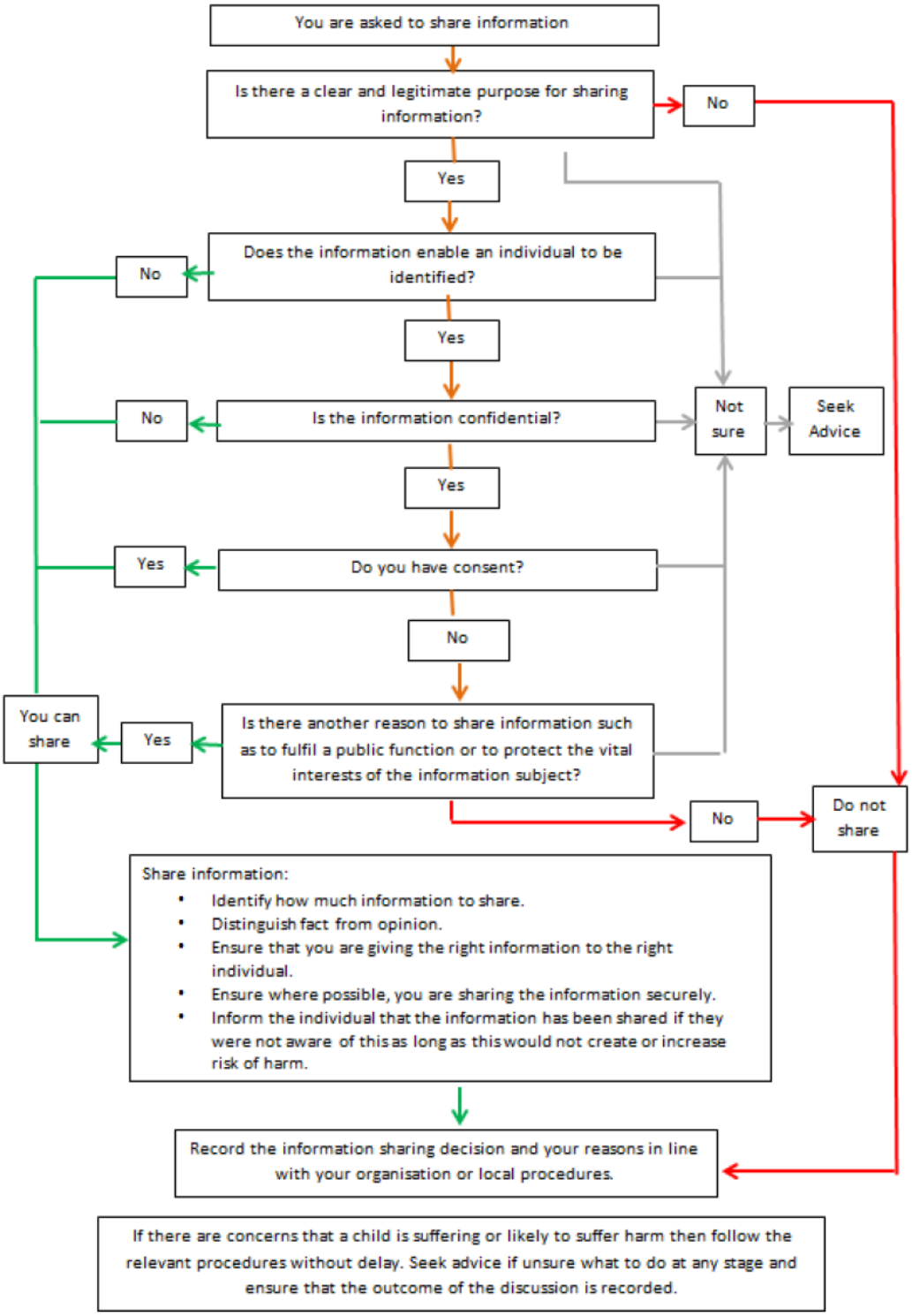
• where practitioners need to share special category personal data, they should be aware that the Data Protection Act 2018 includes 'safeguarding of children and individuals at risk' as a condition that allows practitioners to share information **without consent**

• information **can be shared legally without consent**, if a practitioner is unable to, cannot be reasonably expected to gain consent from the individual, or if to gain consent could place a child at risk.

• relevant personal information can be shared lawfully if it is to keep a child or individual at risk safe from neglect or physical, emotional or mental harm, or if it is protecting their physical, mental, or emotional well-being.

Source:
Information sharing - Advice for practitioners providing safeguarding services to children, young people, parents and carers - July 2018 – HM Government

Flowchart of when and how to share information



Source:
Information sharing - Advice for practitioners providing safeguarding services to children, young people, parents and carers - July 2018 – HM Government