Abbey Court School

LOCATION : SCHOOL HANDBOOK, SECTION 1, DOCUMENT 40

MEDWAY COUNCIL

EDUCATION DEPARTMENT

DATA PROTECTION POLICY
(INCLUDING GENERAL DATA PROTECTION REGULATIONS)

First adopted by the Governing Body, October 2018
Approved by the Governing Body, October 2018

This policy was last reviewed to ensure appropriateness and relevance in September 2018

Data Protection Policy

(updated for GDPR May 2018)

Description:	This document outlines the school's policy on data protection, in line with updated GDPR Regulations (25th May 2018)
Policy Audience:	Staff, Pupils, Parents & Carers
Other related school policies and procedures:	For example: Equality Policy, Safeguarding / Child Protection Policy / Computing Policy
Policy last updated for GDPR:	September 2018
Ratified by Full Governing Body:	October 2018
Frequency of review:	Every two years
Date for next review:	Autumn 2019

Data Protection Policy (GDPR Update)

Contents

1. AIMS

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, volunteers, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION & GUIDANCE

This policy meets the requirements of the GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR, the ICO's code of practice for Subject Access Requests and guidance material published by The Department for Education (DfE).

This policy also reflects the ICO's code of practice for the use of CCTV, surveillance cameras and personal information.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

3. DEFINITIONS

Term: Personal Data.

Definition: Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.

Term: Special categories of personal data.

Definition: Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation.

Term: Processing.

Definition: Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Term: Data subject.

Definition: The identified or identifiable individual whose personal data is held or processed.

Term: Data controller.

Definition: A person or organisation (school) that determines the purposes and the means of processing of personal data.

Term: Data processor.

Definition: A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Term: Personal data breach.

Definition: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. THE DATA CONTROLLER

Our school processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller. The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. ROLES & RESPONSIBILITIES

This policy applies to **all staff employed** by our school, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 Governing Body

The governing body has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

5.2 Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing body and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO and, where applicable, Subject Access Requests.

Our DPO's contact details are below:

Contact Name: Andy Wilson

Contact Address: via Abbey Court School

Contact Email: office@abbeycourt.medway.sch.uk

Contact Telephone: 01634 338220

5.3 HEADTEACHER

The Headteacher / Principal acts as the representative of the data controller on a day-to-day basis.

5.4 ALL STAFF

Staff are responsible for:

• Collecting, storing and processing any personal data in accordance with this policy

• Informing the school of any changes to their personal data, such as a change of address

• Contacting the DPO in the following circumstances:

a) With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.

b) If they have any concerns that this policy is not being followed.

c) If they are unsure whether or not they have a lawful basis to use personal data in a particular way.

d) Whenever they are engaging in a new activity or project that may affect the privacy rights of the individual.

e) If there has been a data breach.

f) If they need support / guidance with any contracts or sharing personal data with third parties or transferring personal data outside the European Economic Area.

g) If they need to rely on or capture consent, draft Privacy Notices or deal with data protection rights invoked by an individual.

6. DATA PROTECTION PRINCIPLES

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

• Processed lawfully, fairly and in a transparent manner.

• Collected for specified, explicit and legitimate purposes.

• Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

• Accurate and, where necessary, kept up to date.

• Kept for no longer than is necessary for the purposes for which it is processed.

• Processed in a way that ensures it is appropriately secure.

This policy sets out how the school aims to comply with these principles.

7. COLLECTING PERSONAL DATA

Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

• The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.

• The data needs to be processed so that the school can comply with a legal obligation.

• The data needs to be processed to ensure the vital interests of the individual e.g. to protect someone's life.

• The data needs to be processed so that the school, as a public authority, can perform a task in the public interest, and carry out its official functions.

• The data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden).

• The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.1 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Information and Records Management Society's toolkit for schools.

8. SHARING PERSONAL DATA

We will not normally share personal data with anyone else, but may do so where:

• There is an issue with a pupil or parent/carer that puts the safety of our staff at risk

• We need to liaise with other agencies – we will seek consent as necessary before doing this

• Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:

a) Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law.

b) Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.

c) Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

• The prevention or detection of crime and/or fraud.

• The apprehension or prosecution of offenders.

• The assessment or collection of tax owed to HMRC.

• In connection with legal proceedings.

• Where the disclosure is required to satisfy our safeguarding obligations.

• Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided.

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the school holds about them. This includes:

• Confirmation that their personal data is being processed.

• Access to a copy of the data.

• The purposes of the data processing.

• The categories of personal data concerned.

• Who the data has been, or will be, shared with.

• How long the data will be stored for, or if this isn't possible, the criteria used to determine this period.

• The source of the data, if not the individual.

• Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

Subject Access Requests must be submitted in writing, either by letter, email or fax to the DPO. They should include:

• Name of individual.

• Correspondence address.

• Contact number and email address.

• Details of the information requested and clearly dated.

If staff receive a Subject Access Request they must immediately forward it to the DPO.

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a Subject Access Request with respect to their child, the child must either be unable to understand their rights and the implications of a Subject Access Request, or have given their consent.

Children below the age of 12 (Primary Schools) are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above (Secondary Schools) are generally regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents or carers of pupils at our school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

• May ask the individual to provide 2 forms of identification.

• May contact the individual via phone to confirm the request was made.

• Will respond without delay and within 1 month of receipt of the request.

• Will provide the information free of charge.

• May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary.

We will not disclose information if it:

• Might cause serious harm to the physical or mental health of the pupil or another individual.

• Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests.

• Is contained in adoption or parental order records.

• Is given to a court in proceedings concerning the child.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other data protection rights of the individual

In addition to the right to make a Subject Access Request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

• Withdraw their consent to processing at any time.

• Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).

• Prevent use of their personal data for direct marketing.

• Challenge processing which has been justified on the basis of public interest.

• Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

• Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them).

• Prevent processing that is likely to cause damage or distress.

• Be notified of a data breach in certain circumstances.

• Make a complaint to the ICO.

• Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. PARENTAL REQUESTS TO SEE THE EDUCATIONAL RECORD

Parents may make a request to see their child's educational record. This request must be made in writing to the Headteacher / Principal via the school office.

11. BIOMETRIC RECOGNITION SYSTEMS

If and where the School uses pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). If a biometric system is introduced we will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish.

Parents/carers and pupils can object to participation in a school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

The School may use CCTV in various locations around the school site to ensure it remains safe. If we use CCTV we will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Data Protection Officer (DPO).

13. PHOTOGRAPHS & VIDEOS

As part of our school activities, we may take photographs and record images of individuals within our school.

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Uses may include:

• Within school on notice boards and in school magazines, brochures, newsletters, etc.

• Outside of school by external agencies such as the school photographer, newspapers, campaigns.

• Online on our school website or social media pages. We will monitor regularly websites, brochures and display boards to ensure that images of pupils are not used if they have left the school.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

Related school policy: See our Child Protection and Safeguarding Policy for more information on our use of photographs and videos.

14. DATA PROTECTION BY DESIGN & DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

• Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.

• Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6).

• Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process).

• Integrating data protection into internal documents including this policy, any related policies and privacy notices.

• Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance.

• Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

• Maintaining records of our processing activities, including:

a) For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).

b) For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

15. DATA SECURITY & STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

• Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are secure when not in use.

• Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.

• Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals.

• Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices where personal information is stored.

• Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our E-Safety policy on acceptable use).

• Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

16. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

Data is stored and disposed of in line with the IRMS Toolkit for schools (Information and Records Management Society).

17. PERSONAL DATA BREACHES

The school will make all reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

When appropriate, we will report the data breach to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

• A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium.

• Safeguarding information being made available to an unauthorised person.

• The theft of a school laptop containing non-encrypted personal data about pupils.

18. TRAINING

All staff and governors are provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

The school offers online training as appropriate.

19. MONITORING ARRANGEMENTS

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed initially within the first 12 months from the date of this document to ensure that any new updates from ICO, DfE are incorporated. After this initial period this policy will be reviewed every two years and ratified by the Full Governing Body.

20. LINKS WITH OTHER POLICIES

This data protection policy is linked to other policies including:

- Safeguarding / Child Protection Policy.
- E-Safety Policy.
- Staff ICT Code of Conduct and Acceptable Use Agreement.

Karen Joy – September 2018

Appendix 1 – Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

• On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO

• The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:

a) Lost

b) Stolen

c) Destroyed

d) Altered

e) Disclosed or made available where it should not have been

f) Made available to unauthorised people

• The DPO will alert the headteacher and the chair of governors

• The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

• The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen

• The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

a) Loss of control over their data.

b) Discrimination.

c) Identify theft or fraud.

d) Financial loss.

e) Unauthorised reversal of pseudonymisation (for example, key-coding).

f) Damage to reputation.

g) Loss of confidentiality.

h) Any other significant economic or social disadvantage to the individual(s) concerned.

If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

Documented decisions are stored by the DPO electronically and electronic copy held by Headteacher and Chair of Governors for their reference.

• Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:

a) A description of the nature of the personal data breach including, where possible:

- The categories and approximate number of individuals concerned.
- The categories and approximate number of personal data records concerned.

b) The name and contact details of the DPO.

c) A description of the likely consequences of the personal data breach.

d) A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

• If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible

• The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

a) The name and contact details of the DPO.

b) A description of the likely consequences of the personal data breach.

c) A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned

• The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies

• The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

a) Facts and cause.

b) Effects.

c) Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).

Records of all breaches will be stored by the DPO electronically.

• The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

Actions to minimise the impact of data breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

• If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

• Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

• If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it.

• In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.

• The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.

• The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other types of breach that you might want to consider could include:

• Details of pupil premium interventions for named children being published on the school website.

• Non-anonymised pupil exam results or staff pay information being shared with governors.

• A school laptop containing non-encrypted sensitive personal data being stolen or hacked.

• The school's cashless payment provider being hacked and parents' financial details stolen.

Appendix 2 – School Privacy Notices

Abbey Court School

Privacy Notice - how we use pupil information

The categories of pupil information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 1 and phonics results, post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)

This list is not exhaustive, nor limited to the above.

Why we collect and use pupil information

We collect and use pupil information, for the following purposes:

a) to support pupil learning
b) to monitor and report on pupil attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us for DfE data collections
g) to comply with the law regarding data sharing

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing pupil information are: section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We also comply with Article 6 (1)(c) and Article 9 (2)(b) of the General Data Protection Regulation (GDPR).

How we collect pupil information

We collect pupil information via registration/data collection forms at the start of the school year or Common Transfer File (CTF) or secure file transfer from previous schools if applicable.

Pupil data is essential for the schools' operational use. Whilst the majority of pupil information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store pupil data

We hold pupil data securely for the set amount of time shown in our data retention schedule. Data will be retained for all pupils enrolled at the school until the age of 25, after which they will be safely destroyed.

Who we share pupil information with

We routinely share pupil information with:

- schools/colleges that the pupils attend after leaving us
- our local authority (Medway)
- youth support services (pupils aged 13+)
- the Department for Education (DfE)
- NHS and health care professionals

Why we regularly share pupil information

We do not share information about our pupils with anyone without consent, unless the law and our policies allow us to do so.

We share pupils' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

Youth support services

Pupils aged 13+

Once our pupils reach the age of 13, we also pass pupil information to our Local Authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child/pupil once they reach the age 16 where applicable.

Pupils aged 16+

We will also share certain information about pupils aged 16+ with our Local Authority and/or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.

This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

For more information about services for young people, please visit our Local Authority website.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and Local Authorities via various statutory data collections. We are required to share information about our pupils with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under: section 3 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact Karen Joy, Headteacher. The school will, on an annual basis, share individual Data Collection Sheets with you in order to ensure that records are accurate and up to date.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/.

Contact

If you would like to discuss anything in this privacy notice, please contact:
Karen Joy, Headteacher or Andy Wilson, Data Protection Officer.

How Government uses your data

The pupil data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

Much of the data about pupils in England goes on to be held in the National Pupil Database (NPD).

The NPD is owned and managed by the Department for Education and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.

It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.

To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department

The law allows the Department to share pupils' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit: https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 pupils per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares

To contact DfE: https://www.gov.uk/contact-dfe

Abbey Court School

Privacy Notice - how we use workforce information

The categories of school information that we process include:

- personal information (such as name, date of birth, employee or teacher number, national insurance number, address, telephone and e-mail contact details, car registration)
- special categories of data needed for the Disclosure and Barring Service and Single Central Register (such as DBS number, right to work in the UK, convictions/cautions)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, employee reference number, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- relevant medical information (such as health clearance information, occupational health reports)
- other information to support the financial and personnel requirements of the school.

Why we collect and use workforce information

We collect and use staff information under the EU General Data Protection Regulation (GDPR).

We use workforce data to:

a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) to comply with the law regarding checks such as DBS and medical clearance
e) submit annual statistical returns to Central Government

Under the General Data Protection Regulation (GDPR), the legal basis/bases we rely on for processing personal information for general purposes are set out in Article 6 of the GDPR and Article 9 (Special Category Data). Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

Collecting workforce information

We collect personal information via PMC001 and Staff Data Collection forms. Workforce data is essential for the school's/Local Authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. Data will not be kept for longer than is necessary. The school follows the Information Commissioner's guidance on retention of documents, including the Information and Records Management Society's Retention Guidelines for School.

Who we share workforce information with

We routinely share this information with:

- our Local Authority (where applicable)
- the Department for Education (DfE)
- another establishment when an employment reference has been requested

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so. Workforce data is shared with the Local Authority via the completion of Human Resource/Payroll forms to enable contracts to be created and staff to be paid on a regular basis. Workforce data is routinely collected by Central Government every Autumn by the school submitting a Workforce Census Return through the SIMS database to enable statistical analysis to be undertaken at a National level.

Local authority

We are required to share information about our workforce members with our Local Authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and Local Authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current government security policy framework.

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact Karen Joy, Headteacher.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact Karen Joy, Headteacher or Andy Wilson, Data Protection Officer.

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

Sharing by the Department

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

Appendix 3 - Information Sharing

HM Government

Information sharing

Advice for practitioners providing safeguarding services to children, young people, parents and carers

July 2018

Contents

Summary

Information sharing is essential for effective safeguarding and promoting the welfare of children and young people. It is a key factor identified in many serious case reviews (SCRs), where poor information sharing has resulted in missed opportunities to take action that keeps children and young people safe.

About this government advice

This HM Government advice is non-statutory, and has been produced to support practitioners in the decisions they take to share information, which reduces the risk of harm to children and young people and promotes their well-being.

This guidance does not deal in detail with arrangements for bulk or pre-agreed sharing of personal information between IT systems or organisations other than to explain their role in effective information governance.

This guidance has been updated to reflect the General Data Protection Regulation (GDPR) and Data Protection Act 2018, and it supersedes the HM Government *Information sharing: guidance for practitioners and managers* published in March 2015.

Who is this advice for?

This advice is for all frontline practitioners and senior managers working with children, young people, parents and carers who have to make decisions about sharing personal information on a case-by-case basis. It might also be helpful for practitioners working with adults who are responsible for children who may be in need.

The seven golden rules to 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.

Sharing Information

Sharing information is an intrinsic part of any frontline practitioners' job when working with children and young people. The decisions about how much information to share, with whom and when, can have a profound impact on individuals' lives. Information sharing helps to ensure that an individual receives the right services at the right time and prevents a need from becoming more acute and difficult to meet.

Poor or non-existent information sharing is a factor repeatedly identified as an issue in Serious Case Reviews (SCRs) carried out following the death of or serious injury to, a child. In some situations, sharing information can be the difference between life and death.

Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children at risk of abuse or neglect. Every practitioner must take responsibility for sharing the information they hold, and cannot assume that someone else will pass on information, which may be critical to keeping a child safe.

Professor Munro's review of child protection concluded the need to move towards a child protection system with less central prescription and interference, where we place greater trust in, and responsibility on, skilled practitioners at the frontline.[1] Those skilled practitioners are in the best position to use their professional judgement about when to share information with colleagues working within the same organisation, as well as with those working within other organisations, in order to provide effective early help, to promote their welfare, and to keep children safe from harm.

Lord Laming emphasised that the safety and welfare of children is of paramount importance and highlighted the importance of practitioners feeling confident about when and how information can be legally shared.[2] He recommended that all staff in every service, from frontline practitioners to managers in statutory services and the voluntary sector should understand the circumstances in which they may lawfully share information, and that it is in the public interest to prioritise the safety and welfare of children.

Being alert to signs of abuse and neglect and taking action

All practitioners should be alert to the signs and triggers of child abuse and neglect.[3] Abuse (emotional, physical and sexual) and neglect can present in many different forms. Indicators of abuse and neglect may be difficult to spot. Children may disclose abuse, in

---

[1] The Munro review of child protection: final report – a child centred system

[2] The Protection of Children in England: a progress plan

[3] What to do if you're worried a child is being abused

which case the decision to share information is clear, as actions must be taken to respond to the disclosure. In other cases, for example, neglect, the indicators may be more subtle and appear over time. In these cases, decisions about what information to share, and when, will be more difficult to judge. Everyone should be aware of the potential for children to be sexually exploited for money, power, or status, and individuals should adopt an open and inquiring mind to what could be underlying reasons for behaviour changes in children of all ages.

If a practitioner has concerns about a child's safety or welfare, they should share the information with the local authority children's social care, NSPCC and/or the police, in line with local procedures. Security of information sharing must always be considered and should be proportionate to the sensitivity of the information and the circumstances. If it is thought that a crime has been committed and/or a child is at immediate risk, the police should be notified immediately.

Legislative framework

Key organisations who have a duty under section 11 of the Children Act 2004 to have arrangements in place to safeguard and promote the welfare of children are:

- the local authority;
- NHS England;
- clinical commissioning groups;
- NHS Trusts, NHS Foundation Trusts;
- the local policing body;
- British Transport Police Authority;
- prisons;
- National Probation Service and Community Rehabilitation Companies;[4]
- youth offending teams; and
- bodies within the education and /or voluntary sectors, and any individual to the extent that they are providing services in pursuance of section 74 of the Education and Skills Act 2008.

[4] The duty under section 11 of the Children Act 2004 will apply to Community Rehabilitation Companies via contractual arrangements entered into by these bodies with the Secretary of State under Section 3 of the Offender Management Act 2007.

There are also a number of other similar duties, which apply to other organisations. For example, section 175 of the Education Act 2002 which applies to local authority education functions and to governing bodies of maintained schools and further education institutions, and section 55 of the Borders, Citizenship and Immigration Act 2009 which applies to the immigration, asylum, nationality and customs functions of the Secretary of State (in practice discharged by UK Visas and Immigration, Immigration Enforcement and the Border Force, which are part of the Home Office).

Where there are concerns about the safety of a child, the sharing of information in a timely and effective manner between organisations can improve decision-making so that actions taken are in the best interests of the child. The GDPR and Data Protection Act 2018 place duties on organisations and individuals to process personal information fairly and lawfully; they are not a barrier to sharing information, where the failure to do so would cause the safety or well-being of a child to be compromised. Similarly, human rights concerns, such as respecting the right to a private and family life would not prevent sharing where there are real safeguarding concerns.

All organisations should have arrangements in place, which set out clearly the processes and the principles for sharing information internally. In addition, these arrangements should cover sharing information with other organisations and practitioners, including third party providers to which local authorities have chosen to delegate children's social care functions, and any Local Safeguarding Children Board (LSCB) still operating within the local authority area as well as safeguarding partners (please see below).

One approach to aid effective information sharing is the use of Multi-Agency Safeguarding Hubs, where teams may be co-located physically or locally. In these settings, it is important that accountability is defined to ensure that teams know who is responsible for making decisions and that actions taken are in the best interest of the child.

Safeguarding partners (as defined in Section 16E of the Children Act 2004) and LSCBs (where still in operation) should play a strong role in supporting information sharing between and within organisations and addressing any barriers to information sharing. This should include ensuring that a culture of appropriate information sharing is developed and supported as necessary by multi-agency training.

Safeguarding partners and LSCBs (where still in operation) can require a person or body to comply with a request for information, as outlined in sections 16H and 14B of the Children Act 2004, respectively. This can only take place when the information requested is for the purpose of enabling or assisting the safeguarding partners or LSCB to perform their functions. Any request for information to a person or body, should be necessary and proportionate to the reason for the request. Safeguarding partners and LSCBs should be mindful of the burden of requests and should explain why the information is needed.

The principles

The principles set out below are intended to help practitioners working with children, young people, parents and carers share information between organisations. Practitioners should use their judgement when making decisions about what information to share, and should follow organisation procedures or consult with their manager if in doubt.

The most important consideration is whether sharing information is likely to support the safeguarding and protection of a child.

Necessary and proportionate

When taking decisions about what information to share, you should consider how much information you need to release. Not sharing more data than is necessary to be of use is a key element of the GDPR and Data Protection Act 2018, and you should consider the impact of disclosing information on the information subject and any third parties. Information must be proportionate to the need and level of risk.

Relevant

Only information that is relevant to the purposes should be shared with those who need it. This allows others to do their job effectively and make informed decisions.

Adequate

Information should be adequate for its purpose. Information should be of the right quality to ensure that it can be understood and relied upon.

Accurate

Information should be accurate and up to date and should clearly distinguish between fact and opinion. If the information is historical then this should be explained.

Timely

Information should be shared in a timely fashion to reduce the risk of missed opportunities to offer support and protection to a child. Timeliness is key in emergency situations and it may not be appropriate to seek consent for information sharing if it could cause delays and therefore place a child or young person at increased risk of harm. Practitioners should ensure that sufficient information is shared, as well as consider the urgency with which to share it.

Secure

Wherever possible, information should be shared in an appropriate, secure way. Practitioners must always follow their organisation's policy on security for handling personal information.

Record

Information sharing decisions should be recorded, whether or not the decision is taken to share. If the decision is to share, reasons should be cited including what information has been shared and with whom, in line with organisational procedures. If the decision is not to share, it is good practice to record the reasons for this decision and discuss them with the requester. In line with each organisation's own retention policy, the information should not be kept any longer than is necessary. In some rare circumstances, this may be indefinitely, but if this is the case, there should be a review process scheduled at regular intervals to ensure data is not retained where it is unnecessary to do so.

When and how to share information

When asked to share information, you should consider the following questions to help you decide if, and when, to share. If the decision is taken to share, you should consider how best to effectively share the information. A flowchart follows the text.

When

Is there a clear and legitimate purpose for sharing information?

- Yes – see next question
- No – do not share

Do you have consent to share?

- Yes – you can share but should consider how
- No – see next question

Does the information enable an individual to be identified?

- Yes – see next question
- No – you can share but should consider how

Have you identified a lawful reason to share information without consent?

- Yes – you can share but should consider how
- No – do not share

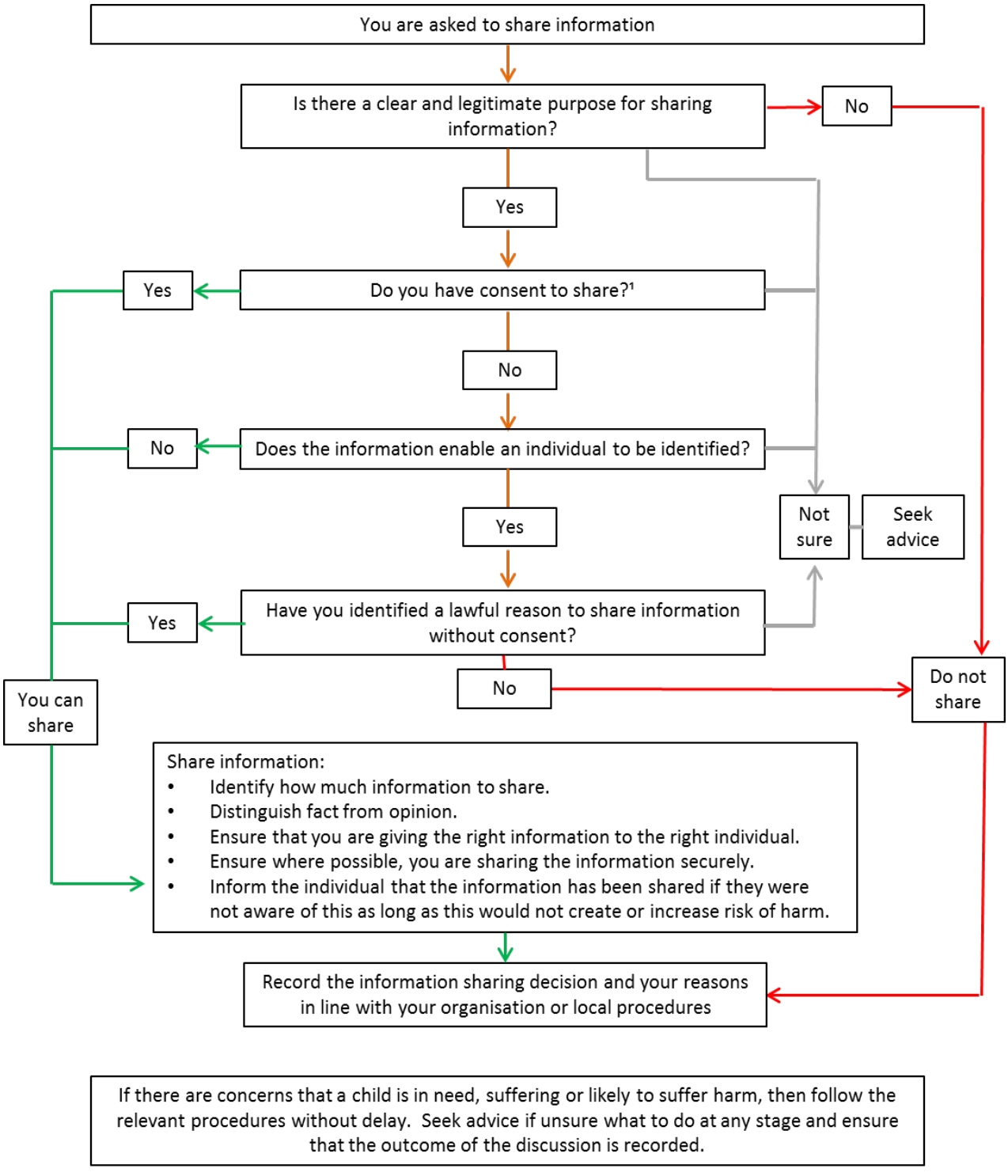
How

- Identify how much information to share
- Distinguish fact from opinion
- Ensure that you are giving the right information to the right individual
- Ensure where possible that you are sharing the information securely
- Where possible, be transparent with the individual, informing them that that the information has been shared, as long as doing so does not create or increase the risk of harm to the individual.

All information sharing decisions and reasons must be recorded in line with your organisation or local procedures. If at any stage you are unsure about how or when to

share information, you should seek advice on this. You should also ensure that the outcome of the discussion is recorded.

Flowchart of when and how to share information



1. Consent must be unambiguous, freely given and may be withdrawn at any time

Myth-busting guide

Sharing of information between practitioners and organisations is essential for effective identification, assessment, risk management and service provision. Fears about sharing information cannot be allowed to stand in the way of the need to safeguard and promote the welfare of children and young people at risk of abuse or neglect. Below are common myths that can act as a barrier to sharing information effectively:

The GDPR and Data Protection Act 2018 are barriers to sharing information

No – the GDPR and Data Protection Act 2018 do not prohibit the collection and sharing of personal information. They provide a framework to ensure that personal information is shared appropriately. In particular, the Data Protection Act 2018 balances the rights of the information subject (the individual whom the information is about) and the possible need to share information about them. Never assume sharing is prohibited – it is essential to consider this balance in every case. You should always keep a record of what you have shared.

Consent is always needed to share personal information

No – you do not necessarily need the consent of the information subject to share their personal information.

Wherever possible, you should seek consent and be open and honest with the individual from the outset as to why, what, how and with whom, their information will be shared. You should seek consent where an individual may not expect their information to be passed on. When you gain consent to share information, it must be explicit, and freely given.

There may be some circumstances where it is not appropriate to seek consent, either because the individual cannot give consent, it is not reasonable to obtain consent, or because to gain consent would put a child or young person's safety or well-being at risk.

Where a decision to share information without consent is made, a record of what has been shared should be kept.

Personal information collected by one organisation cannot be disclosed to another organisation

No - this is not the case, unless the information is to be used for a purpose incompatible with the purpose it was originally collected for. In the case of children in need, or children at risk of significant harm, it is difficult to foresee circumstances where information law would be a barrier to sharing personal information with other practitioners.

Practitioners looking to share information should consider which processing condition in the Data Protection Act 2018 is most appropriate for use in the particular circumstances of the case. This may be the safeguarding processing condition or another relevant provision.

The common law duty of confidence and the Human Rights Act 1998 prevent the sharing of personal information

No - this is not the case. In addition to the GDPR and Data Protection Act 2018, practitioners need to balance the common law duty of confidence, and the rights within the Human Rights Act 1998, against the effect on children or individuals at risk, if they do not share the information.

If information collection and sharing is to take place with the consent of the individuals involved, providing they are clearly informed about the purpose of the sharing, there should be no breach of confidentiality or breach of the Human Rights Act 1998. If the information is confidential, and the consent of the information subject is not gained, then practitioners need to decide whether there are grounds to share the information without consent. This can be because it is overwhelmingly in the information subject's interests for this information to be disclosed. It is also possible that a public interest would justify disclosure of the information (or that sharing is required by a court order, other legal obligation or statutory exemption).

In the context of safeguarding a child or young person, where the child's welfare is paramount, it is possible that the common law duty of confidence can be over overcome. Practitioners must consider this on a case-by-case basis. As is the case for all information processing, initial thought needs to be given as to whether the objective can be achieved by limiting the amount of information shared – does all of the personal information need to be shared to achieve the objective?

IT Systems are often a barrier to effective information sharing

No – IT systems, such as the Child Protection Information Sharing project (CP-IS), can be useful in supporting information sharing. IT systems are most valuable when practitioners use the data that has been shared to make more informed decisions about how to support and safeguard a child. Evidence from the Munro Review is clear that IT systems will not be fully effective unless individuals from organisations co-operate around meeting the needs of the individual child. Professional judgment is the most essential aspect of multi-agency work, which could be put at risk if organisations rely too heavily on IT systems.

Useful resources and external organisations

- The Information Commissioner's Office (ICO) website
- Practice guidance on sharing adult safeguarding information

Other relevant departmental advice and statutory guidance

- Working Together to Safeguard Children (2018)
- Keeping Children Safe in Education (2016)
- What to do if you're worried a child is being abused (2015)

HM Government

About this publication:

enquiries www.education.gov.uk/contactus

download www.gov.uk/government/publications

Reference: DFE-00128-2018

Follow us on Twitter:
@educationgovuk

Like us on Facebook:
facebook.com/educationgovuk