Middlestone Moor Primary School

Data Protection Policy

July 2020

To be reviewed: July 2021 by Data Protection Officer

1. Aims & Objectives

The aim of this policy is to provide a framework to enable staff, parents, pupils, governors and visitors to understand:

- the law regarding personal data
- how personal data should be processed, stored, archived and disposed of
- the rights in respect of people whose data is being held and processed by the school (this includes pupils, parents, staff and governors).

As a school we aim to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018)

1.1. Safeguarding

The Data Protection Act 2018 and GDPR do not prevent, or limit, the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to promote the welfare and protect the safety of children.
Keeping children safe in Education
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

1.2. It is a statutory requirement for our school to have a Data Protection Policy:

http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/a00201669/statutory-policies-for-schools

In addition to this policy, our school also has:

- **Record Keeping and Retention Policy** - details on how long all records are retained
- **Information Asset Register** - a comprehensive audit listing all the information that the school holds, who has access to the information and the legal basis for processing it
- **Privacy Notices -** for pupils, parents, staff and governors
- **Registered with the ICO**

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

It also reflects the ICO's code of practice for the use of 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.

2.1. Definitions

TERM	DEFINITION
Personal data	Any information relating to an identified, or identifiable, living 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.
Special categories of personal data	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
Processing	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.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

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

2.2. Data Protection Principles

Article 5 of the GDPR sets out that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, subject to measures respecting the principle of 'data minimisation', not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. School take steps to ensure information, such as parental contact details, are updated regularly

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals, and again subject to the 'data minimisation' principle; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

In addition, Article 5(2) requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles. In effect the school, as the 'data controller', needs to be able to show that its policies and systems comply with requirements of GDPR.

3. Lawfulness, fairness and transparency

We will only process personal data where we have one of the 6 'lawful bases' to do so as stipulated under GDPR and data protection law. The vast majority of information that school collects and processes is required to enable the school to perform tasks carried out in the public interest or in the exercise of official authority

vested in the school, as the data controller. Our legal basis for processing information is detailed in our Information Asset Register.

The lawful bases from which school can operate under are;

- 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school performs as a public authority) 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 under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **explicit consent**
- The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for the establishment, exercise or defence of **legal claims**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation
- The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given **consent**
- The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made **manifestly public** by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights**
- The data needs to be processed for reasons of **substantial public interest** as defined in legislation

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

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

4. 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.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate.

In addition, 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 school's record retention schedule.

5. Age

Children under the age of 13 are not usually considered able to give consent to process data or to directly access the rights of a data subject, so parents or guardians can do this on their behalf, providing this is in the best interests of the child. See https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-rights-do-children-have/ Children are provided with age appropriate advice about how their data is used.

6. Consent

If there is a lawful basis for collecting data, then consent to collect data is not required. (An employee could not opt to withhold an NI number for example.) However, a privacy notice which explains to data subjects (or the parents of the data subject if under the age of 13) will be required. This explains the lawful basis for processing the data, and also explains to the individual their rights.

Parents/Carers or children over the age of 13 will need to give consent when there is not a legal reason for processing, for instance for images used in school publicity or social media feeds. The consent will need to be transparent, revocable, and will need to be on an "Opt-in" basis.

7. Rights

GDPR provides the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Different rights attach to different lawful bases of processing:

	Right to erasure	**Right to portability**	**Right to object**
Vital Interests	✓	**X**	**X**
Legal Obligation	**X**	**X**	**X**
Public Task	**X**	**X**	✓
Legitimate Interests	✓	**X**	✓
Contract	✓	✓	**X**
Consent	✓	✓	**X** but right to withdraw consent

a. **The right to be informed – see Privacy Notices**
b. **The right of access**
   Depending on the age of the pupil, there are two legal basis for pupils or parents to request access to their data – a Subject Access Request or a request under the 2005 Education Regulations.

   i. Subject Access request under GDPR

GDPR gives individuals the right to access any data that an organisation holds on them. Therefore, 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a subject access request in any form they must immediately forward it to the DPO.

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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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 may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

Further guidance is available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

School is aware that guidance from the ICO highlights the rights of the child. *"Before responding to a subject access request for information held about a child, you should consider whether the child is mature enough to understand their rights. If you are confident that the child can understand their rights, then you should usually respond directly to the child. You may, however, allow the parent to exercise the child's rights on their behalf if the child authorises this, or if it is evident that this is in the best interests of the child."*

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, some 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.

In maintained schools, parents or those with parental responsibility have another statutory right to access their children's educational record.

This is part of the Education (Pupil Information) Regulations 2005. This applies to all children under 18 years and has to be completed in 15 working days. See https://ico.org.uk/your-data-matters/schools/pupils-info/. There are certain circumstances in which this right can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

c. The right to erasure

GDPR includes a right to erasure – but this is not an absolute right and does not necessarily override the lawful basis for continuing to hold data. School's legal advisor will support with information about which data can continue to be legally held if a data

subject asks to be 'forgotten'. Our data management systems such as SIMS will begin to improve their functionality to either delete or anonymise personal data when appropriate.

It will be seen from the table above that, where school relies on either a 'legal obligation' or a 'public task' basis for processing (see above), there is no right to erasure – however, this does not mean the data will never be erased. It will still not be retained for any longer than necessary, in accordance with statutory requirements and/or our data retention guidelines which are set out in our Record Keeping and Retention Policy.

Other Data Protection Rights of the individuals

In addition to the right to make a subject access request, erasure (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 or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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.

8. Data Types

Not all data needs to be protected to the same standards - the more sensitive or potentially damaging the loss of the data is, the better it needs to be secured. There is inevitably a compromise between usability of systems and working with data. In a school environment staff are used to managing risk, for instance during a PE or swimming lesson where risks are assessed, controlled and managed. A similar process should take place with managing school data. GDPR defines different types of data and prescribes how it should be treated.

The loss or theft of any Personal Data is a "Potential Data Breach", which could result in legal action against the school. The loss of sensitive, or "special category", personal data is considered much more seriously and the sanctions may well be more punitive.

a. Personal data

The school has access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the school community – including pupils-/students, members of staff and parents/carers e.g. names, addresses, contact details, legal guardianship contact details, disciplinary records
- Curricular/academic data e.g. class lists, pupil/student progress records, reports, references
- Professional records e.g. employment history, taxation and national insurance records, appraisal records, disciplinary records and references
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

b. Special Category Data

"Special Category Data" are data revealing a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data, data concerning a person's health or sexual life is prohibited except in special circumstances.

This is because special category data is more sensitive, and so needs more protection.

In our school the most likely special category data is likely to be:

- information on the racial or ethnic origin of a pupil or member of staff
- information about the sexuality of a child, his or her family or a member of staff
- medical information about a child or member of staff (SEND)
- (some information regarding safeguarding will also fall into this category)
- staffing e.g. Staff Trade Union details.

Note – See section on Sharing Information.

c. Other types of Data not covered by the act

This is data that does not identify a living individual and, therefore, is not covered by the remit of the DPA - this may fall under other 'access to information' procedures. This would include Lesson Plans (where no individual pupil is named), Teaching Resources and other information about the school which does not relate to an individual. Some of this data would be available publicly (for instance the diary for the forthcoming year), and some of this may need to be protected by the school. We may choose to protect some data in this category but there is no legal requirement to do so.

9. 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.

9.1 Governing Body

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

9.2 Data protection officer

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 board 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.

Our DPO is Darren Hobson and is contactable via email at info@mobile-sbm.com or by telephone on 07850060027

9.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

9.4 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:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

9.5 Risk management - Staff and Governors Responsibilities

Everyone in the school has the responsibility of 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.

10. Photographs and 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.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school newsletters, brochures etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on our school website or social media pages

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.

See our Photographic and Video Policy for more information on our use of photographs and videos.

11. Data protection by design and 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 data protection 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

- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- Maintaining records of our processing activities, including:
  - 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)
  - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how we are keeping the data secure

12. Legal Requirements

a. Registration

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner and each school is responsible for their own registration: https://ico.org.uk/for-organisations/data-protection-fee The register may be checked by visiting https://ico.org.uk/about-the-ico/what-we-do/register-of-fee-payers/

b. Information for Data Subjects (Parents, Staff): PRIVACY NOTICES

In order to comply with the fair processing requirements of the DPA, the school **must** inform parents/carers of all pupils/students and staff of the data they collect, process and hold on the pupils/students, the purposes for which the data is held, the legal basis for holding it and the third parties (e.g. LA, DfE, etc) to whom it may be passed. The privacy notice will also need to set out the data subjects' rights under the GDPR. More information about the suggested wording of privacy notices can be found on the DfE website: http://www.education.gov.uk/researchandstatistics/datatdatam/a0064374/pn

Privacy notices will be made available to pupils, parents and carers, by publishing on the school website and making a paper copy available when children first register for school.

Children will be provided with age appropriate information about how their data is being used.

13. Transporting, Storing and Disposing of personal Data

a. Information security - Storage and Access to Data

The more sensitive the data the more robust the security measures will need to be in place to protect it.

i. Technical Requirements

The school will ensure that IT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the

role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Personal data may only be accessed on machines that 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 for five minutes.

All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.

Personal data can only be stored on school equipment (this includes computers, the Cloud and portable storage media (where allowed). Private equipment (ie owned by the users) must not be used for the storage of personal data.

The school has clear policy and procedures for the automatic backing up, accessing and restoring all data held on school systems, including off-site backups.

ii. Portable Devices

When personal data is stored on any portable computer system, USB stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected)
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete
- Only encrypted removable storage purchased by the school is allowed to be used on school computers.

iii. Passwords

All users will use strong passwords (14 Characters including a Capital letter, number and symbol) which must be updated regularly. User passwords must never be shared – this includes with agency staff or students. It is advisable NOT to record complete passwords, but prompts could be recorded.

iv. Images

Images will be protected and stored in a secure area. See school Photographic Policy.

v. Cloud Based Storage

The school has clear policy and procedures for the use of “Cloud Based Storage Systems” (for example Dropbox, Google Apps and Onedrive) and is aware that data held in remote and cloud storage is still required to be protected in line with the Data Protection Act. The school will ensure that it is satisfied with controls put in place by

remote/cloud based data services providers to protect the data. See advice from the DfE below: https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

b. Third Party data transfers

As a Data Controller, the school is responsible for the security of any data passed to a "third party". Data Protection clauses will be included in all contracts where data is likely to be passed to a third party, as well as data processing agreements.

c. Retention of Data

The school have a Record Keeping and Retention Policy in place which sets out how long data and information is to be retained.

d. Systems to protect data

vi. Paper Based Systems

All paper based personal data will be protected by appropriate controls, for example:

- paper based safeguarding chronologies will be in a locked cupboard when not in use
- class lists used for the purpose of marking may be stored in a teacher's bag.

Paper based personal information sent to parents will be double checked by another member of staff before sending.

vii. School Websites

Uploads to the school website will be checked prior to publication, for instance:

- to check that appropriate photographic consent has been obtained
- to check that the correct documents have been uploaded.

viii. E-mail

E-mail cannot be regarded on its own as a secure means of transferring personal data.

Where technically possible, all e-mail containing sensitive information will be encrypted by the sender. If members of staff are unsure how to encrypt emails they will seek advice from the school's ICT Technician. Methods of encryption include attaching the sensitive information as a word document and encrypting the document/compressing with 7 zip and encrypting - the recipient will then need to contact the school for access to a one-off password [*or when available* using the security features available in Office 365).

15. 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.

All staff will ensure they follow the school's procedures for deletion of paper records. Paper should be shredded using a cross-cutting shredder; CDs / DVDs / diskettes should be cut into pieces. Hard-copy images, Audio Visual recordings and hard disks should be dismantled and destroyed. Where third party disposal experts are used they should ideally be supervised but, in any event, under adequate contractual obligations to the school to process and dispose of the information securely. Whenever records are destroyed, staff should record the details blow on the school's Data deletion log which is held by the school office:

- File reference (or other unique identifier)
- File title (or brief description)
- No of files
- The name of the authorising officer
- Date of destruction

16. Data Sharing

We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations 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:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service

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

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 internationally, we will do so in accordance with data protection law. Other specific examples are;

Sharing with the LA and DfE

The school is required by law to share information with the LA and DfE. Further details are available at: https://www.gov.uk/guidance/data-protection-how-we-collect-and-share-research-data

Safeguarding

Schools MUST follow the statutory processes in Keeping Children safe in Education and Working together to Safeguard Children https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Durham LSCB provides information on information sharing at: http://www.durham-lscb.org.uk/wp-content/uploads/sites/29/2016/06/Guide-for-professionals-on-information-sharing.pdf

Transfer of Safeguarding and SEND records when a pupil moves school

The following is an extract from keeping Children safe in Education Sept 2018.

- Where children leave the school or college, the designated safeguarding lead should ensure their child protection file is transferred to the new school or college as soon as possible, ensuring secure transit, and confirmation of receipt should be obtained. For schools, this should be transferred separately from the main pupil file.

- Receiving schools and colleges should ensure key staff such as designated safeguarding leads and SENCOs or the named person with oversight for SEN in a college, are aware as required.

- In addition to the child protection file, the designated safeguarding lead should also consider if it would be appropriate to share any information with the new school or college in advance of a child leaving. For example, information that would allow the new school or college to continue supporting victims of abuse and have that support in place for when the child arrives.

.

17. Data Breach – Procedures

On occasion, personal data may be lost, stolen or compromised. The data breach includes both electronic media and paper records, and it can also mean inappropriate access to information.

- In the event of a data breach, the data protection officer will inform the head teacher and chair of governors.
- When a personal data breach has occurred, the DPO must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk, then the DPO must notify the ICO; if it's unlikely then it need not be reported to the ICO. However, if the school decide not to report the breach, they need to be able to justify this decision, and it should be documented.
- The DPO must report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the DPO takes longer

than this, they must give reasons for the delay. It is important therefore that any member of staff causing a data breach or being aware of a date breach inform the DPO immediately.

- If a breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR states you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO.

Any report about a data breach must include:

- a description of the nature of the personal data breach including, where possible:
    - the categories and approximate number of individuals concerned; *and*
    - the categories and approximate number of personal data records concerned;
- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; *and*
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach including, where appropriate, the measures taken to mitigate any possible adverse effects.

Further details are available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

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.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the full governing body.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme

E-Safety policy

Acceptable use policy

CCTV policy

Child protection and safeguarding policy

Photographic and video policy

Record keeping and retention policy

Data breach procedure

Appendix 1 - Links to Resources and Guidance

ICO Guidance
Specific information for schools is available here. This includes links to guides from the DfE.
http://ico.org.uk/for_organisations/sector_guides/education

Specific Information about CCTV.
https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Information and Records Management Society – schools records management toolkit
A downloadable schedule for all records management in schools.
http://irms.org.uk/page/SchoolsToolkit

Disclosure and Barring Service (DBS)
Details of storage and access to DBS certificate information.
https://www.gov.uk/government/publications/handling-of-dbs-certificate-information/handling-of-dbs-certificate-information

DFE
GDPR Toolkit
https://www.gov.uk/government/publications/data-protection-toolkit-for-schools

Privacy Notices
https://www.gov.uk/government/publications/data-protection-and-privacy-privacy-notices

Use of Biometric Data
https://www.gov.uk/government/publications/protection-of-biometric-information-of-children-in-schools

Safeguarding
https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
and
https://www.gov.uk/government/publications/working-together-to-safeguard-children--2

Appendix 2 - Glossary

GDPR - The General Data Protection Regulation. These are new European-wide rules that are the basis of data protection legislation. They are enforced in the UK by the ICO.

Data Protection Act 1998: Now superseded by GDPR
All personal data which is held must be processed and retained in accordance with the eight principles of the Act and with the rights of the individual. Personal data must not be kept longer than is necessary (this may be affected by the requirements of other Acts in relation to financial data or personal data disclosed to Government departments). Retention of personal data must take account of the Act, and personal data must be disposed of as confidential waste. Covers both personal data relating to employees and to members of the public.

ICO:
The Information Commissioner's Office. This is a government body that regulates the Data Protection Act and GDPR
The ICO website is here http://ico.org.uk/

Data Protection Act 1998: Compliance Advice. Subject access – Right of access to education records in England:
General information note from the Information Commissioner on access to education records. Includes timescale (15 days) and photocopy costs.

Data Protection Act 1998: Compliance Advice. Disclosure of examination results by schools to the media:
General information note from the Information Commissioner on publication of examination results.

Education Act 1996:
Section 509 covers retention of home to school transport appeal papers. (By LA)

Education (Pupil Information) (England) Regulations 2005:
Retention of Pupil records

Health and Safety at Work Act 1974 & Health and Safety at Work Act 1972: Retention requirements for a range of health and safety documentation including accident books, H&S manuals etc.

School Standards and Framework Act 1998:
Retention of school admission and exclusion appeal papers and other pupil records.

Appendix 3

Subject Access Request Procedure

Individuals can submit a subject access request (SAR) to the school in any form. There are designated forms that can be filled in for such requests and these are available in school. However, requests can also be made verbally or in writing in other formats, for example via email.

The school may need to undertake checks where necessary on the identity of the individual making the request before releasing the information if this is not clear.

The process to be followed in the event of a member of staff receiving a SAR is as follows;