



Data Protection Policy.

Version	4
Name of Policy writer	Gill Smith
Last Updated	August 2026
Review Date	
Approved	September 2026
ICO registration number	Z6959236

Contents

1	Policy statement
2	About this policy
3	Definition of data protection terms
4	Data Controller
5	Data Protection Officer
6.	Our Data Protection Commitments
7	Roles and Responsibilities across Name of Trust/Academy/School
8	Data protection principles
9	Legal grounds for processing
10	Processing for limited purposes
11	Notifying data subjects
12	Adequate relevant and non-excessive
13	Accurate data
14	Timely processing
15	Processing in line with data subject's rights
16	Data security
17	Personal Data Breaches
18	Data Protection Impact Assessments/Data Protection by design and default
19	Disclosure and sharing of personal information
20	Data processors
21	Biometric Recognition Systems
22	Images and videos
23	CCTV
24	Training
25	Complaints
25	Changes to this policy
Appendix 1 - Definition of terms	
Appendix 2a - Procedures relating to Individual's rights	
Appendix 2b - Responding to a Subject Access Request (SAR)	
Appendix 2c - Record of Information Request	
Appendix 3 - Personal Data Breach Procedures	

1 Policy statement

- a. Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities at Gaskell CP School we will collect, store and **process personal data** about our pupils, **workforce**, parents and others. This makes us a **data controller** in relation to that **personal data**.
- b. We are committed to the protection of all **personal data** and **special category personal data** for which we are the **data controller** and this policy sets out how we comply with relevant legislation. Breaches of this policy can result in risk of real harm to individuals, action for damages, loss of trust and reputational harm as well as regularity penalties, including fines.
- c. The law imposes significant fines for failing to lawfully **process** and safeguard **personal data** and failure to comply with this policy may result in those fines being applied.
- d. All members of our **workforce/data users** must comply with this policy when **processing personal data** on our behalf. Any breach of this policy may result in disciplinary or other action. Individuals may be prosecuted for committing offences under sections 170-173 of the Data Protection Act 2018.
- e. At Gaskell CP School our data protection ethos connects legal privacy rules to our core values of respect, safety and trust. It ensures that the handling of student and staff information reflects an environment where personal dignity is valued and rights are protected. We treat personal details with care, respect and dignity because every person matters. We want to be open, clear and honest with families about why information is gathered and how it is used. We want to ensure that there is a shared responsibility where we expect all staff, helpers and leaders to guard private details on a day-to-day basis.

About this policy

- a. The types of **personal data** that we may be required to handle include information about pupils, parents, our **workforce**, and others that we deal with. The **personal data** which we hold is subject to certain legal safeguards specified in the General Data Protection Regulation ('**GDPR**'), the Data Protection Act 2018, and other regulations (together '**Data Protection Legislation**').
- b. This policy and any other documents referred to in it set out the basis on which we will **process** any **personal data** we collect from **data subjects**, or that is provided to us by **data subjects** or other sources.
- c. This policy does not form part of any employee's contract of employment and may be amended at any time.
- d. This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.
- e. It meets the requirements of GDPR and the provisions of the Data Protection Act 2018. It is based on guidance published by the **Information Commissioner (IC)**. It also reflects the IC'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 Definition of data protection terms

- a. All defined terms in this policy are indicated in **bold** text, and a list of definitions is included in Appendix 1 to this policy.

3 Data Controller

- a. Gaskell CP School processes personal data relating to pupils, parents, staff, governors, visitors and others and is therefore a Data Controller

- b. Gaskell CP School is registered as a **Data Controller** with the **ICO** and will renew this registration annually or as is otherwise legally required

4 **Data Protection Officer**

- a. At Gaskell CP School we are required to appoint a **Data Protection Officer (DPO)**. Our **DPO** is Gill Smith and they can be contacted at gill@mindography.co.uk
- b. The **DPO** is responsible for informing and advising Gaskell CP School about Data Protection Legislation, ensuring compliance with the law and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the **DPO**.
- c. The **DPO** is also the central point of contact for all **data subjects**, the **Information Commission (IC)** and others in relation to matters of data protection.

5 **Our data protection commitments**

- a. We are dedicated to ensuring that **personal data** is processed in alignment with the legal principles of data protection.
- b. We implement a strategy focussed on “Data Protection by Design and Default”.
- c. We can prove our adherence to **data protection legislation**.
- d. **Data subjects** are well informed about how and why we use their data, and how they can exercise their rights regarding their data.
- e. We share **personal data** only when it is fair and lawful, ensuring that any data sharing is conducted securely.
- f. We handle and report all **personal data breaches**, including minor ones, effectively to mitigate any potential risks and to improve our practices.

6 **Roles and responsibilities**

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

- a. **Governing Board** – The Governing Board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.
- b. **Data Protection Officer** - see section 5.
- c. **Sarah Barlow** The Head Teacher acts as the representative of the **Data Controller** on a day-to-day basis. The Head Teacher is responsible for ensuring that their school is compliant to data protection laws. The Head Teacher will delegate duties throughout the school to ensure that correct processes and procedures are undertaken to meet the requirements of com
- d. **All Staff** - Staff are responsible for:
 - I. Collecting, storing and processing any **personal data** in accordance with this policy
 - II. Informing the school of any changes to their **personal data**, such as a change of address
 - III. Contacting the **DPO** in the following circumstances:
 - IV. With any questions about the operation of this policy, data protection law, retaining **personal data** or keeping **personal data** secure
 - V. If they have any concerns that this policy is not being followed
 - VI. If they are unsure whether or not they have a lawful basis to use **personal data** in a particular way
 - VII. 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

- VIII. If there has been a data breach/suspected data breach/near miss
- IX. Whenever they are engaging in a new activity that may affect the **privacy rights of individuals**
- X. If they need help with any contracts or sharing **personal data** with third parties
- XI. If they would like training or awareness sessions arranged for themselves or colleagues

- e. Gaskell CP School ensure that all staff (including contract, temporary, third party and supply staff) are given the correct information from the offset on our expectations of staff in terms of data protection. All staff work in a “data safe” culture. We implement this mind-set to help make staff aware that any action that they do that comes into contact with personal data is done in such a way to protect a data subject’s personal data.

7 Data protection principles

- a. Anyone **processing personal data** must comply with the data protection principles. **We will comply with these principles in relation to any processing of personal data by the school. The principles provide that personal data must be:**
- b. **processed** fairly and lawfully and transparently in relation to the **data subject**. **This means that we only use personal data with respect for the individual to whom it relates, in line with legal grounds for processing and we inform data subjects how their data is processed including, among other ways, in our privacy notices**
- c. **processed** for specified, **explicit and lawful** purposes and in a way which is not incompatible with those purposes. **This means that if we collect data for one purpose and then need to use it for another reason we will ensure that the new purpose is compatible with the original reason for processing**
- d. adequate, relevant and not excessive for the purpose. **This means that we will collect enough information to achieve our aim, whilst minimising that collection to what is genuinely required**
- e. accurate and up to date. **This means that we will try to ensure that data is accurate when we collect it, and kept up-to-date over time**
- f. not kept for any longer than is necessary for the purpose. **This means that we only keep personal data for as long as it is necessary and we comply with our Data Retention Policy**
- g. **processed** securely using appropriate technical and organisational measures. **Our measures include technical safeguards like security of ICT systems, control over ICT access, the use of pseudonyms and encryption as well as organisations safeguards including plans for business continuity, securing our premises and data physically, implementing policies and procedures, conducting regular training and carrying out audits and evaluations of operational measures and strategic oversight of compliance**
- h. Personal data must also:
 - I. be **processed** in line with **data subjects'** rights
 - II. not be transferred to people or organisations situated in other countries without adequate protection.

8 Legal grounds for processing

- a. Data Protection Legislation is not intended to prevent the **processing of personal data**, but to ensure that it is done fairly and without adversely affecting the rights of the **data subject**.
- b. For **personal data** to be **processed** fairly, **data subjects** must be made aware:
 - I. that the **personal data** is being **processed**
 - II. why the **personal data** is being **processed**

- III. what the lawful basis is for that **processing** (see below)
 - IV. whether the **personal data** will be shared, and if so with whom
 - V. the period for which the **personal data** will be held
 - VI. the existence of the **data subject's** rights in relation to the **processing** of that **personal data**
 - VII. the right of the **data subject** to raise a complaint with the **Information Commissioner** in relation to any **processing**.
 - VIII. We will only obtain such **personal data** as is necessary and relevant to the purpose for which it was gathered, and will ensure that we have a lawful basis for any **processing**.
- c. For **personal data** to be **processed** lawfully, it must be **processed** on the basis of one of the legal grounds set out in the Data Protection Legislation. We will normally **process personal data** under the following legal grounds:
- I. where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract
 - II. where the **processing** is necessary to comply with a legal obligation that we are subject to
 - III. where the **processing** is necessary in order to protect the vital interests of a **data subject** or another individual
 - IV. where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest
 - V. where the **processing** is necessary for the purposes of our recognised legitimate interest as set out in Annex 1 of the **GDPR**
 - VI. where the processing is necessary for the purposes of our legitimate interests (or the legitimate interests of a third party) except where such interests are overridden by the interests and fundamental rights and freedoms of the **data subject**
 - VII. where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data**
- d. When **special category personal data** is being processed then an additional legal ground must apply to that processing. We will normally only **process special category personal data** under following legal grounds:
- I. where the **processing** is necessary for employment law purposes, for example in relation to sickness absence
 - II. where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment
 - III. where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities
 - IV. where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **special category personal data**.
- e. We will inform **data subjects** of the above matters by way of appropriate **privacy notices** which shall be provided to them when we collect the data or as soon as possible thereafter, unless we have already provided this information such as at the time when a pupil joins us.

- f. If any **data user** is in doubt as to **the legal ground for processing**, then they must contact the DPO before doing so.

Vital Interests

- g. There may be circumstances where it is considered necessary to **process personal data** or **special category personal data** in order to protect the vital interests of a **data subject**. This might include medical emergencies where the **data subject** is not in a position to give consent to the **processing**. We believe that this will only occur in very specific and limited circumstances. In such circumstances we would usually seek to consult with the DPO in advance, although there may be emergency situations where this does not occur.

Consent

- h. Where none of the other bases for **processing** set out above apply then the school must seek the consent of the **data subject** before **processing** any **personal data** for any purpose.
- i. There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.
- j. When pupils and/or our **workforce** join Gaskell CP School a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, among other things. Where appropriate third parties may also be required to complete a consent form.
- k. In relation to all pupils **aged 12 years and under** we will seek consent from an individual with parental responsibility for that pupil.
- l. We will generally seek consent directly from a pupil who **is aged 13 years and over**, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from an individual with parental responsibility.
- m. If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:
 - a. inform the **data subject** of exactly what we intend to do with their **personal data**
 - b. require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in
 - c. inform the **data subject** of how they can withdraw their consent.
- n. Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a **data subject** giving their consent. **We will ensure that it will be as easy for the data subject to withdraw their consent as it was to give it**
- o. The **DPO** must always be consulted in relation to any consent form before consent is obtained.
- p. A record must always be kept of any consent, including how it was obtained and when.

10 Processing for limited purposes

- a. In the course of our activities as a school we may collect and **process** the **personal data** set out in our Record of Data Processing Activities. This may include **personal data** we receive directly from a **data**

subject (for example, by completing forms or by corresponding with us by mail, phone, email or otherwise) and **personal data** we receive from other sources (including, for example, local authorities, other schools, parents, other pupils or members of our **workforce**).

- b. We will only **process personal data** for the specific purposes set out in our **Record of Data Processing Activities** or for any other purposes specifically permitted by Data Protection Legislation or for which specific consent has been provided by the data subject.
- c. The **Record of Data Processing Activities** will be reviewed on an at least annual basis by Shabana Yusuf although some sections may be delegated to and reviewed by other members of staff. It will also be reviewed when a significant change to data processing occurs and in line with recommendations made in any **DPIAs** (see section 18).
- d. The **Record of Data Processing Activities** is a comprehensive overview of how we organise and process **personal data**. It includes information on Gaskell CP School's function, the purpose of processing, names and contact details of joint controllers (if applicable), categories of **data subjects**, categories of personal data, with whom the data may be shared, contracts with third party data processors, international transfers (if applicable), **retention schedules**, technical and organisational security measures, lawful basis for processing, **rights of the individual**, whether automated decision making has been used, the source of the **personal data**, access arrangements and whether any **DPIAs** have been completed.

11 Notifying data subjects

- a. If we collect **personal data** directly from **data subjects**, we will inform them about:
 - i. our identity and contact details as **Data Controller** and those of the **DPO**
 - ii. the purpose or purposes and legal basis for which we intend to **process** that **personal data**
 - iii. the types of third parties, if any, with which we will share or to which we will disclose that **personal data**
 - iv. whether the **personal data** will be transferred outside the European Economic Area ('EEA') and if so the safeguards in place
 - v. the period for which their **personal data** will be stored, by reference to our **Retention Schedule** – in our Information Management and Retention Policy
 - vi. the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making
 - vii. the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the **Information Commissioner**.
- b. Unless we have already informed **data subjects** that we will be obtaining information about them from third parties (for example in our privacy notices), then if we receive **personal data** about a **data subject** from other sources, we will provide the **data subject** with the above information as soon as possible thereafter, informing them of where the **personal data** was obtained from.
- c. Gaskell CP School may be provided with information relating to third parties in the form of emergency contact details. Parents/**carers** are required to obtain the consent of any third party whose details they provide to Gaskell CP School for these purposes. Privacy Notices detailing how the information will be stored and used can be accessed through the Name of Gaskell CP School.

12 Adequate, relevant and non-excessive processing

- a. We will only collect **personal data** to the extent that it is required for the specific purpose notified to the **data subject**, unless otherwise permitted by Data Protection Legislation.

13 Accurate data

- a. We will ensure that **personal data** we hold is accurate and kept up to date.
- b. We will take reasonable steps to destroy or amend inaccurate or out-of-date data.
- c. **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

14 Timely processing

- a. We will not keep **personal data** longer than is necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy, or erase from our systems, all **personal data** which is no longer required.
- b. Gaskell CP School will maintain a **data retention and disposal schedule** which is an annual review of school records and data destruction which aligns with our **retention schedule (in our Information Management and retention Policy)**.
- c. Shabana Yusuf Business Manager is responsible for ensuring that this annual review takes place and that the Annual Review of School Records and Data Destruction checklist is completed. Some sections may be delegated to specific members of staff/roles.

15 Processing in line with data subject's rights

- a. In addition to the right to be informed and the right to withdraw consent, we will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:
 - I. request access to any **personal data** we hold about them
 - II. object to the **processing** of their **personal data**, including the right to object to direct marketing
 - III. have inaccurate or incomplete **personal data** about them rectified
 - IV. restrict **processing** of their **personal data**
 - V. have **personal data** we hold about them erased
 - VI. object to the making of decisions about them by automated means.
- b. The right available to **data subjects** will depend on the lawful basis for **processing**, for example where **personal data** is **processed** under the lawful basis of public task, then the **data subject** cannot withdraw consent for such **processing**, but they exercise the right of objection.
- c. Except for the right to object to direct marketing, other rights requests in an education or employment context can be complex. We will comply with our obligations under **data protection laws** and the guidance given by the **IC** in respect of individuals seeking to exercise their rights.
- d. We will consider **data subject** requests and provide a response within one month, except if we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.

- e. Where we are unable to grant **data subjects** any requests made as part of their rights, for example, where we are unable to delete data as we are required to retain it in relation any claim or legal proceedings, we will explain to the **data subject** of their right to complain to the **IC** at the time that we inform them of our decision in relation to their request.
- f. The **DPO** must be consulted in relation to any **data subject rights request**.

The Right of Access to Personal Data

- g. **Subject Access Requests (SAR)** - Data subjects may request access to all **personal data** we hold about them. Such requests will be considered in line with Gaskell CP School's **Subject Access Request** Procedure. This procedure is available at [W Procedures for dealing with a SAR.docx](#) "Making a Subject Access Request".
- h. 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
- i. **Subject Access Requests** can be either verbal or in writing (letter or email). To ensure greatest clarity it is preferred that such requests are made in writing. must be submitted in writing. They should include:
 - Name of individual
 - Correspondence address
 - Contact number and email address
 - Details of the information requested
 - How the requestee would like the information to be shared with them (e.g. paper or electronic format)
- j. If staff receive a subject access request, they must immediately forward it to the DPO or Shabana Yusuf. (See Appendix 2 for Procedures relating to **Individual Rights**)
- k. **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.
- l. Children aged 12 years and under 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.
- m. If a young person is aged 13 years and over and is felt to have the maturity and competency to understand the request and the nature of the information that will be shared their authorisation should be sought to check that they are happy for their personal data to be shared with their parent/carers. Where we have requested authorisation, the one month time period will not begin until the date the authorisation is received.
- n. **Responding to Subject Access Requests** - When responding to requests, we:
 - May ask the individual to provide 2 forms of identification. We are not required to process any **SAR** until we are satisfied with the individual's identity in order to avoid the potential for an inadvertent disclosure of **personal data** resulting in a data breach. Where we have requested ID the one month time period will not begin until the date the ID is received
 - May contact the individual via phone to confirm the request was made

- Will respond without delay and within 1 calendar month from the date of receipt of the request. We will calculate the time period from the day we receive the request (whether it is a working day or not) until the corresponding day of the next month. If the corresponding calendar date in the next month is a weekend or bank holiday, we will have until the next working day to respond.
 - Will provide the information free of charge
 - There are certain circumstances where we can extend the time period for responding to a SAR by up to 3 months from the date the request is received. We will inform the individual of this within 1 month and explain why the extension is necessary. Examples of when this may occur are when:
 - A request is complex where there are large amounts of sensitive information and there is a need to carefully consider applicable exemptions and redaction
 - Where there are technical difficulties in retrieving the information
 - Where we need to obtain specialist legal advice
 - Where we need to clarify issues surrounding disclosure of information about a child to a parent or legal guardian.
- o. We will not disclose information if it:
- Might cause detriment, 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 (e.g. if there have been allegations of abuse or safeguarding concerns)
 - Is contained in adoption or parental order records
 - Is given to a court in proceedings concerning the child
 - Conflicts when a duty of confidence is owed to the child
 - Conflicts if any views the child or young person has on whether their parents, guardians or authorised representatives should have access to information about them.
- p. **Clarifying requests** - if we are unsure about what information has been requested, or it is apparent that information is not likely to be accessible via a reasonable and proportionate search, we may ask the requester to specify the information their request relates to before responding to the request (e.g. by asking if there are specific dates they are referring to , or any specific incidents on which they wish to focus). If we seek clarification from the requester, the time limit for responding to the request will be paused until the clarification is provided.
- q. 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; if the requester clearly has no intention of exercising their right of access; if the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption; if the requester makes unsubstantiated accusations against specific employees which are clearly promoted by malice. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the IC.
- r. Under the Education (Pupil Information) (England) Regulations 2005 a parent/carers can request to see their child's **educational record**, or request it on behalf of their child, in writing. This right applies regardless of the age of the child. The information will be presented within 15 school days of receiving the request. There will be no charge for the information requested.

The Right to Object

- s. In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.
- t. An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.
- u. Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.
- v. In respect of direct marketing any objection to **processing** must be complied with.
- w. Gaskell CP School is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

The Right to Rectification

- x. If a **data subject** informs Gaskell CP School that **personal data** held about them by Gaskell CP School is inaccurate or incomplete then we will consider that request and provide a response within one month.
- y. If we consider the issue to be too complex to resolve within that period then we may extend the response period by a further two months. If this is necessary then we will inform the **data subject** within one month of their request that this is the case.
- z. We may determine that any changes proposed by the **data subject** should not be made. If this is the case then we will explain to the **data subject** why this is the case. In those circumstances we will inform the **data subject** of their right to complain to the **IC** at the time that we inform them of our decision in relation to their request.

The Right to Restrict Processing

- aa. **Data subjects** have a right to 'block' or suppress the **processing** of **personal data**. This means that Gaskell PC School can continue to hold the **personal data** but not do anything else with it.
- bb. Gaskell CP School must restrict the **processing** of **personal data**:
 - I. where it is in the process of considering a request for **personal data** to be rectified (see above)
 - II. Where Gaskell CP School is in the process of considering an objection to processing by a **data subject**
 - III. where the **processing** is unlawful but the **data subject** has asked Gaskell CP school not to delete the **personal data**
 - IV. Where Gaskell CP School no longer needs the **personal data** but the **data subject** has asked Gaskell CP School not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against Gaskell CP School.
- cc. If Gaskell CP School has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.
- dd. The DPO must be consulted in relation to requests under this right.

The Right to Be Forgotten

- ee. **Data subjects** have a right to have **personal data** about them held by Gaskell CP School erased only in the following circumstances.
- I. Where the **personal data** is no longer necessary for the purpose for which it was originally collected.
 - II. When a **data subject** withdraws consent – which will apply only where Gaskell CP School is relying on the individuals consent to the **processing** in the first place.
 - III. When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object.
 - IV. Where the **processing** of the **personal data** is otherwise unlawful.
 - V. When it is necessary to erase the **personal data** to comply with a legal obligation.
- ff. Gaskell CP School is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:
- I. to exercise the right of freedom of expression or information
 - II. to comply with a legal obligation for the performance of a task in the public interest or in accordance with the law
 - III. for public health purposes in the public interest
 - IV. for archiving purposes in the public interest, research or statistical purposes
 - V. in relation to a legal claim.
- gg. If Gaskell CP School has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.
- hh. The DPO must be consulted in relation to requests under this right.

Right to Data Portability

- ii. In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to another organisation.
- jj. If such a request is made then the DPO must be consulted.

16 Data security

- a. We will take appropriate security measures against unlawful or unauthorised processing of **personal data**, and against the accidental loss of, or damage to, **personal data**.
- b. We will put in place procedures and technologies to maintain the security of all **personal data** from the point of collection to the point of destruction.
- c. Security procedures include:

- ii. **Entry controls.** Any stranger seen in entry-controlled areas should be reported to the main School Reception.
 - iii. **Secure lockable desks and cupboards.** Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
 - iv. **Methods of disposal.** Paper documents should be shredded. Digital storage devices should be physically destroyed when they are no longer required. IT assets must be disposed of in accordance with the **IC** guidance on the disposal of IT assets.
 - v. **Equipment. Data users** must ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.
 - vi. **Working away from the school premises – paper document.** Guidance procedures are available for staff
 - vii. **Working away from the school premises – electronic working.** Guidance procedures are available for staff
 - viii. **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.
- d. Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

17 Personal Data Breaches

- a. Gaskell CP School will make all reasonable endeavours to ensure that there are no data breaches and aim to ensure that all personal data that we hold is protected to the highest possible standard.
- b. We are aware that data breaches may occur **despite our policies, procedures and measures in place to protect personal data and we will respond to any breach as quickly as possible in order to minimise any risks or potential harm to individuals.**
- c. **We have a thorough data breach action plan to manage if/when a data breach occurs. Procedures are set out in Appendix 3.**
- d. 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 a school website which shows the exam results of pupils eligible for 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 Data Protection Impact Assessments/Data Protection by design and default

- a. Gaskell CP School takes data protection very seriously and will consider and comply with the requirements of Data Protection Legislation in relation to all of its activities whenever these involve the use of personal data, in accordance with the principles of data protection by design and default.
- b. In certain circumstances the law requires us to carry out detailed assessments of proposed **processing in a Data Protection Impact Assessment (DPIA)**. This includes where we intend to use new technologies which might pose a high risk to the rights of **data subjects** because of the types of data we will be **processing** or **there is a change in our existing ways of working.**

- c. Gaskell CP School will complete a **DPIA** of any such proposed **processing at the procurement stage and prior to any processing taking place** and has a template document which ensures that all relevant matters are considered. **We may also carry out a DPIA where one is not legally required, as a matter of good practice.**
- d. The **DPO** should always be consulted as to whether a **DPIA** is required, and if so how to undertake that assessment. **The DPO must always be consulted where personal data is to be transferred to different countries to ensure adequate protection is in place.**
- e. **We carry out and review DPIAs in accordance with our proforma and procedures.**
- d. **The Record of Data Processing Activities will be updated in line with any recommendations made as part of a DPIA to reflect the new data processing.**

19 Disclosure and sharing of personal information

- a. We may share **personal data** that we hold about **data subjects**, and without their consent, with other organisations. Such organisations include the Department for Education, [and / or Education and Skills Funding Agency ESFA], Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.
- b. **The Trust/Academy/School will inform data subjects of any sharing of their personal data unless we are not legally required to do so, for example, where personal data is shared with the police in the investigation of a criminal offence**
- c. **Where necessary we will enter into data sharing agreements to help facilitate the safe sharing of personal data.** 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 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
 - 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
- d. In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.
- e. 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.
- f. 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.

20 Data processors

- a. We contract with various organisations who provide services to Gaskell CP School. **These include people, companies and systems that process personal data on behalf and under our instruction.** These are detailed within the Record of Data Processing Activities and privacy notices.
- b. In order that these services can be provided effectively we are required to transfer **personal data of data subjects** to these **data processors**.
- c. **Personal data** will only be transferred to a **data processor** if they agree to comply with our procedures and policies in relation to data security, or if they put in place adequate measures themselves to the satisfaction of Gaskell CP School will always undertake due diligence of any **data processor** before transferring the **personal data of data subjects** to them.

- d. Contracts with **data processors** will comply with **Data Protection Legislation** and contain explicit obligations on the **data processor** to ensure compliance with the **Data Protection Legislation**, and compliance with the rights of **Data Subjects**.

Under the context of the Protection of Freedoms Act 2020 a “child” means a person under the age of 18.

- a. Where we use pupils’ biometric data as part of an automated biometric recognition system (for example, pupils use their finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.
- b. Prior to the use of biometric data a **DPIA** must be conducted.
- c. Parents/carers will be notified before any biometric recognition system is put in place. Gaskell CP School will get written consent from at least one parent or carer before we take any biometric data from their child and first process is Gaskell CP School will use an ‘opt in’ system for collecting consent. Parents/carers and pupils have the right to choose not to use the School’s biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. Parents/carers can withdraw consent at any time and any relevant data already captured will be correctly erased and no longer processed.
- d. Where staff members or other adults use the School’s biometric system(s), we will also obtain their consent before it is first used. Alternative means of accessing the relevant service will be offered if consent is not given. Staff and other adults can also withdraw consent at any time and the School will delete any relevant data already captured.

21 Images and videos

- a. Parents and others attending Gaskell CP School events **are allowed to** take photographs and videos of those events for **personal and** domestic purposes. For example, parents can take video recordings of a school performance involving their child. Gaskell CP School does not prohibit this as a matter of policy.
- b. Gaskell CP School does not however agree to any such photographs or videos being used for any other purpose, but acknowledges that such matters are, for the most part, outside of the ability of the Gaskell CP School to prevent.
- c. Gaskell CP School asks that parents and others do not post any images or videos which include any child other than their own child on any social media or otherwise publish those images or videos.
- d. **When a pupil begins their attendance at Gaskell CP School they, or their parent where appropriate, will be asked to complete a consent form in relation to the use of images and videos of that pupil. Images and videos of pupils may be required for safeguarding procedures and identification and for teaching, learning and assessment purposes and we will not seek consent for the taking and use of these images. We may also take photos and videos of children for school community and celebratory purposes which may be viewed only by our school community. Our lawful basis for processing is “public task”. Consent cannot be withheld for this but there is the right to “object” which can be discussed with Gaskell CP School I. However, as Gaskell CP School we want to celebrate the achievements of our pupils and therefore may want to use images and videos of our pupils within promotional materials, or for publication in the media such as local, or even national, newspapers covering school events or achievements. We will seek the consent of pupils, and their parents where appropriate, before allowing the use of images or videos of pupils for such purposes.**
- f. For our primary schools we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. **Consent is for the duration of a child’s attendance at our school, although this can be withdrawn at any time.**
- g. **For our secondary pupils in Year 7 (younger than 12 years) we will be seeking parental consent for photographs and videos to be taken of pupils for communication, marketing and promotional materials from and parent/carer/guardian and will not ask for consent again. Consent is for the duration of a child’s attendance at our school although this can be withdrawn at any time. In addition, children aged 13 years plus may change**

their consent choices themselves. At Gaskell CP School we discuss photos, online presence and consent with our students as part of PHSE/Life Skills and Wellbeing lessons on digital literacy.

- h. For secondary pupils who start aged 13 years plus we will obtain written consent from the students for photographs and videos to be taken for communication, marketing and promotional materials. Consent is for the duration of a young person's attendance at our school, although this can be withdrawn at any time
- i. If consent is withdrawn, we will delete the photograph/video and not distribute it further. We will also keep on record that consent has been withdrawn for that child so that no further photographs will be used.
- j. 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.

23 CCTV

- a. Gaskell CP School operates a CCTV system. Information held by the school is covered under GDPR; capture of CCTV must be in line with relevant codes of practice including the Surveillance Camera Code of Practice issued by the Surveillance Camera Commissioner, available here:
<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>

and the CCTV Code of Practice issued by the Information Commissioner's Office, available here:
<https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf>

- b. The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.
- c. Surveillance will be used as a deterrent for violent behaviour and damage to the school. The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.
- d. If the surveillance and CCTV systems fulfil their purpose and are no longer required the school will deactivate them.
- e. Gaskell CP School CCTV policy is available on the website  CCTV Policy

24 Training

- a. All staff and governors/trustees are provided with data protection training as part of their induction process.
- b. Data protections will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary. Specific training will be provided for staff who handle personal information and especially special category personal data and/or that is pertinent to their role.
- c. Best practice requires that all staff complete suitable training on an **annual basis**. At Gaskell CP School all staff will complete at least one annual piece of GDPR-related training with half termly refreshers/briefings being discussed at staff meetings.
- d. A record of staff completion of training will be maintained by Shabana Yusuf to ensure that all staff have completed the necessary training

25 Complaints

- a. Data subjects have the right to make a complaint to the school if they consider we have not complied with **data protection legislation** . Any complaints relating to data protection must be directed to our Shabana Yusuf
- b. When dealing with complaints relating to data protection we shall:
 - I. Acknowledge receipt within 30 days of the date on which the complaint is received by Gaskell CP School
 - II. Take appropriate steps to respond to the complaint, including making enquiries into the subject matter of the complaint, to the extent appropriate
 - III. Inform the complainant about progress of the complaint
 - IV. Inform the complainant of the outcome of the complaint
- c. Gaskell CP School have a Data Protection Complaints Policy which can be accessed [Data Protection Complaints Policy with form .docx](#)

26 Changes to this Policy

- a. We may change this policy at any time. Where appropriate we will notify **data subjects** of those changes.

Appendix 1

DEFINITIONS

Term	Definition
Data	Information which is stored electronically, on a computer, or in certain paper-based filing systems.
Data Controllers	The people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with Data Protection Legislation. We are the data controller of all personal data used in our business for our own commercial purposes.
Data Processing Impact Assessment (DPIA)	A DPIA is a process that is carried out in order to assess if data processing is taking place in line with relevant legislation.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
Data Protection Officer (DPO)	A Data Protection Office (DPO) should be appointed when any large-scale processing or data occurs and/or processing of data may be deemed a risk.
Data retention and disposal schedule	This is an annual review of Gaskell CP School's records and data destruction checklist which aligns with the Data Management and Retention Schedule
Data Subjects	For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.
Data Users	Those of our workforce (including governors and volunteers) whose work involves processing personal data. Data users must protect the data they handle in accordance with this data protection policy and any applicable data security procedures at all times.
Personal Data	Any information relating to an identified or identifiable living natural person (a data subject); an identifiable living natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Individual Rights of a Data Subject	Under GDPR there are 8 individual rights (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/): ● Right to be informed ● Right of access ● Right to rectification ● Right to erasure ● Right to restrict processing ● Right to data portability ● Right to object
Information Commission (IC)	In the UK the Information Commission (IC) is the data protection regulator. The website of the IC is at www.ico.org.uk
Privacy Notices	where we collect information either directly or indirectly from data subjects, we provide them with a statement of fair processing, referred to as a privacy notice. This notice will contain information about: our identity and contact details as

	Data Controller and those of the DPO; the purpose or purposes and legal basis for which we intend to process that personal data; the types of third parties, if any, with which we will share or to which we will disclose that personal data; whether the personal data will be transferred outside the UK and if so the safeguards in place; the period for which their personal data will be stored, by reference to our [Data Retention Policy]; the existence of any automated decision making in the processing of the personal data along with the significance and envisaged consequences of the processing and the right to object to such decision making; and the rights of the data subject to object to or limit processing, request information, request deletion of information or lodge a complaint with the IC.
Privacy Rights of the Individual	See Appendix 2a
Processing	Any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring personal data to third parties.
Record of Data Processing Activities or record of Processing Activities (ROPA)	A Record of Data Processing Activities or A Record of Processing Activities (ROPA) is a documented overview of all personal data processing activities an organisation undertakes. It's a key requirement under the General Data Protection Regulation (GDPR) and other data protection laws, designed to demonstrate compliance and accountability.
Retention schedule	The retention and disposal schedule outlines how long records should be kept and how they should be disposed of (This can be found in our Information Management and retention Schedule)
Special Category Personal Data	Information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition or sexual life, or genetic or biometric data.
Subject Access Request (SAR)	This is when a data subject formally lodges a request to view/access the personal data that is held on them.
Workforce	Includes any individual employed by Gaskell CP School such as staff and those who volunteer in any capacity including governors, trustees & members.

Appendix 2a

Procedures relating to the Privacy Rights of an Individual

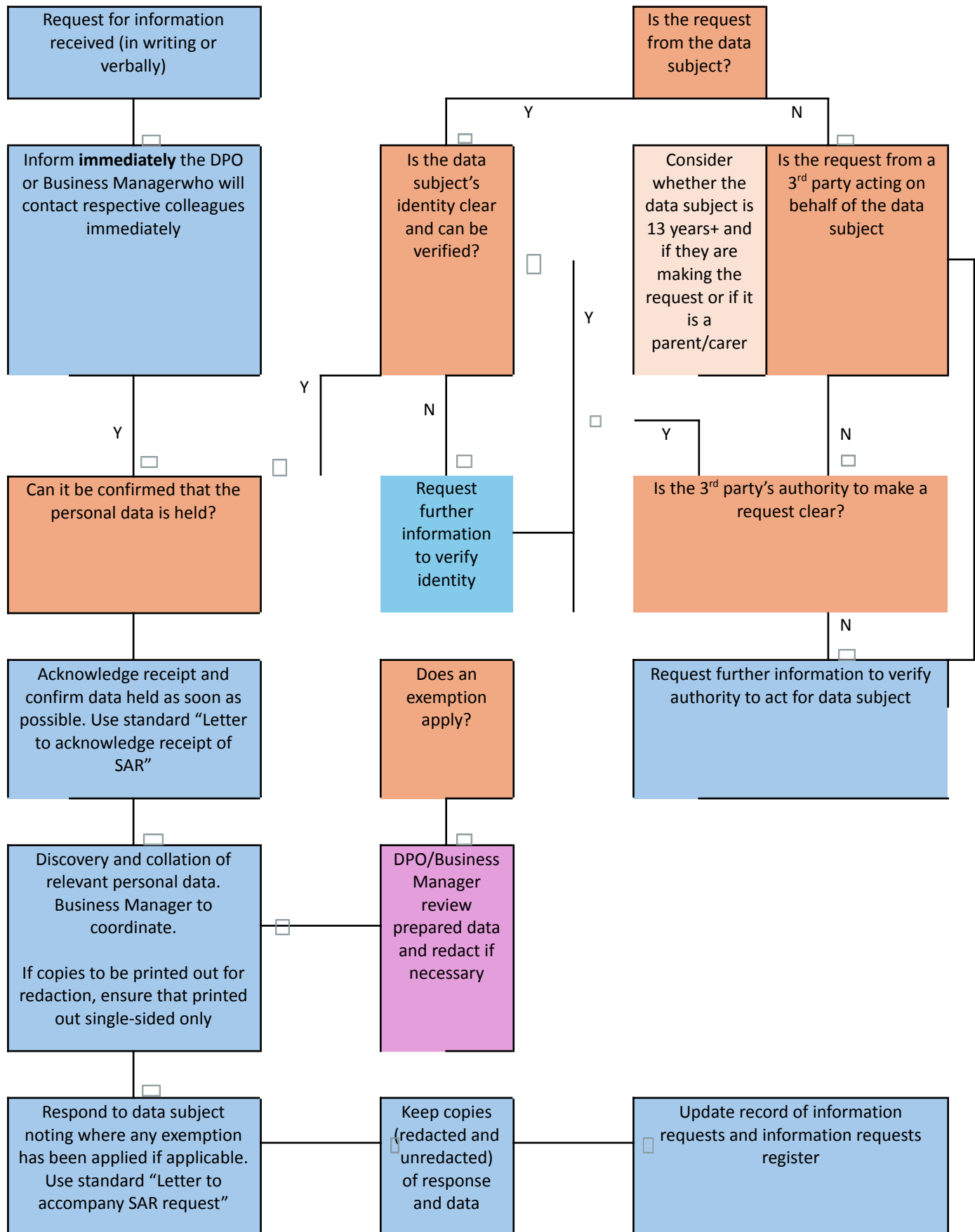
There are 8 Rights for Individuals under GDPR

(<https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/>)

	<u>Summary</u>	<u>Reference in policy</u>
Right to be informed	Individuals have the right to be informed about the collection and used of their personal data	This is included in Privacy Notices
Right of access	Individuals have the right to access and receive a copy of their personal data and other supplementary information. This is often called a Subject Access Request (SAR) See below for school/trust specific procedures	Paragraphs 15 g-s See Appendix 2b
Right to rectification	UK GDR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete	Paragraphs 15 y-aa
Right to erasure/right to be forgotten	Individuals can have their personal data erased	Paragraphs 15 ff-ii
Right to restrict processing	Individuals have the right to request the restation or suppression of their personal data	Paragraphs 15 bb-ee
Right to data portability	The right to data portability allows individuals to obtain reused their personal data for their own purposes across different services	Paragraphs 15 jj-kk
Right to object	UK GDPR gives individuals the right to object to the processing of their personal <u>data in certain circumstances</u>	Paragraphs 15 t-x
Rights related to automated decision-making including profiling		This is included in Privacy Notices

Appendix 2b

Procedures relating to Individual's Rights – responding to a Subject Access Request



Appendix 2c

Record of Information Requests

Type of Information request	Subject Access Request (SAR)		Freedom of Information Request (FOI)		Request by parent to see their child's educational record (N/A for academies)	
Time scale to respond	30 days from receipt		20 school days from receipt		15 school days from receipt	

Please tick appropriate box

Date request received		Response deadline	
Date response sent		Format in which information sent	
Name of requestor		Contact details of requestor	
Name of data subject			

Details of information requested (If SAR details of personal data requested) <i>Copy and paste request</i>			
Identity verified for data subject and requestee if different (e.g. solicitor) (List verification e.g. passport, birth certificate)			
Authorisation given (Form of Authority from YP if 12 years+ or request from 3 rd party)			
Clarification (Has clarification been sought?) <i>If no letter of clarification has been received after 30 days reasonable searches will commence to ensure compliance</i>	Why was clarification sought?		
	Date letter seeking clarification sent		
	Date letter of clarification received		
	New date of response deadline		
	Date any supplementary information has been sent		
If rejected reason for rejection			
If extended deadline, reason for extension			

Any applicable charges	
Redactions <i>(List reasons/exemptions why redactions have been made)</i>	
Response given <i>Copy and paste/add as attachment</i>	

PERSONAL DATA BREACH PROCEDURE

This procedure is based on [guidance on personal data breaches](#) produced by the IC.

- On finding or causing a breach, or potential breach, the staff member or data processor must contain the breach and immediately notify the DPO
- The DPO/GDPR Lead 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:
 - Lost
 - Stolen
 - Destroyed
 - Altered
 - Disclosed or made available where it should not have been
 - Made available to unauthorised people
- The DPO/GDPR Lead will alert the Head Teacher and the Chair of Governors/Trustees
- The DPO/ GDPR Lead 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 IC. 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:
 - Loss of control over their data
 - Discrimination
 - Identify theft or fraud
 - Financial loss
 - Unauthorised reversal of pseudonymisation (for example, key-coding)
 - Damage to reputation
 - Loss of confidentiality
 - 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/most appropriate member of staff/GDPR Lead must notify the IC
- The DPO will document the decision (either way) in case it is challenged at a later date by the IC or an individual affected by the breach. Documented decisions are stored on the school's computer system
- Where the IC must be notified, the DPO/ GDPR Lead will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO/ GDPR Lead will set out:
 - 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
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach

- 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/ GDPR Lead 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/ GDPR Lead expects to have further information. The DPO/ GDPR Lead 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:
 - The name and contact details of the DPO
 - A description of the likely consequences of the personal data breach
 - 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/ GDPR Lead 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 / GDPR Lead will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - Facts and cause
 - Effects
 - 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 on the school's computer system. The DPO/ GDPR Lead and Head Teacher 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 actions 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. Such data breaches 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

For example, if **sensitive information was disclosed via email (including safeguarding records)** the type of actions that could be put in place would be:

- 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/ GDPR Lead 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/ GDPR Lead 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/ GDPR Lead 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