



CLAYESMORE

# DATA PROTECTION POLICY

## (Parent Version)

Responsible:	Head of Compliance
Date Reviewed:	04 February 2024 (Minor Changes)
Review Period:	Annual
Scope:	Whole School
Approval Authority:	Governors
Approval Date:	12/02/2024
External Release:	Yes (Parent Version Only)

# CONTENTS

<b>INTRODUCTION</b>	<b>2</b>
General	2
Scope	2
Data Protection Lead (DPL)	2
<b>GENERAL DATA PROTECTION REGULATION (GDPR)</b>	<b>2</b>
Data Protection Principles	3
The Lawful Basis for Processing Personal Data	3
The Rights of an Individual	3
<b>SAFEGUARDING</b>	<b>5</b>
<b>OUR DATA PROCESSING PRINCIPLES</b>	<b>5</b>
Data Compliance Log	5
Data Audit and Data Subjects	5
<b>USE OF PERSONAL DATA FOR MARKETING AND DEVELOPMENT</b>	<b>6</b>
Electronic Marketing	6
Postal Marketing	6
Obtaining Consent for Using Images	6
<b>PERSONAL DATA IN A HARD COPY FORMAT</b>	<b>6</b>
<b>DATA PROTECTION IMPACT ASSESSMENT (DPIA)</b>	<b>7</b>
<b>PRIVACY NOTICES</b>	<b>7</b>
<b>PROCEDURES FOR THE USE OF IMAGES</b>	<b>8</b>
General Principles	8
Using Images of Pupils	8
Using Images of Staff	8
<b>‘DASH CAM’ USE</b>	<b>9</b>
<b>CCTV SURVEILLANCE SYSTEMS</b>	<b>9</b>
<b>DATA RETENTION REQUIREMENTS</b>	<b>10</b>
<b>DATA BREACHES</b>	<b>11</b>
Dealing with a Data Breach	11
<b>DEALING WITH A SUBJECT ACCESS REQUEST (SAR) OR A REQUEST TO DELETE, RECTIFY OR TRANSFER PERSONAL DATA</b>	<b>12</b>
Data Subject Access Requests	12
<b>DEFINITIONS</b>	<b>14</b>

# INTRODUCTION

## General

Clayesmore School (the School) is a Data Controller as defined within the General Data Protection Regulation (GDPR) legislation, effective 25 May 2018. This means that we determine the purposes and means of processing the personal data that we collect. It is the intent of the school that we should at all times observe, and remain compliant with, the GDPR and any other regulations that may from time to time be introduced into UK legislation. Non-compliance with this policy may be considered a disciplinary offence.

## Scope

This policy replaces all existing specific data protection policies and all references to data protection that may be held within associated documents. It applies to all governors, staff (including volunteers), parents and pupils of Clayesmore Senior and Prep schools and all of those concerned are expected to be familiar with the requirements it places upon them as individuals and on the school generally.

This policy is also applicable to The Clayesmore Society, Friends of Clayesmore, the Old Clayesmorians, Prep Parents Association, Clayesmore Sports Centre and any other society or organisation affiliated to the school, especially those that wish to use the Clayesmore name or brand.

## Data Protection Lead (DPL)

The ICO has not issued a clear position on the requirement to appoint a Data Protection Officer (DPO) within independent schools; the title of DPO has a specific legal meaning within the GDPR. Where the ICO is clear, in which regard ISBA and its lawyers are fully in agreement, is that any school will need to appoint a suitably trained, capable and competent person to take on the role of compliance lead at the organisation. At Clayesmore, this person will be known as the Data Protection Lead (DPL) and is currently integrated into the responsibilities of the Head of Compliance.

## GENERAL DATA PROTECTION REGULATION (GDPR)

The GDPR is a data protection regulation that replaced the Data Protection Act (DPA) 1998 when it came into force on 25 May 2018. The GDPR retains many of the principles contained within the DPA whilst imposing new requirements and provisions to strengthen the rights of individuals to determine how their Personal Data is used. The GDPR applies to both digitally held information and manual 'hard-copy' filing systems.

Personal Data is defined as any information relating to an identifiable person who can be directly or indirectly identified by reference to an 'identifier'. The definition of 'identifier' includes a wide range of information including name, email address, telephone number, identification number, location data or online identifier.

Sensitive Personal Data is a specific type of Personal Data that includes medical and health information, political affiliation, racial or ethnic origin, religious or philosophical beliefs, trade union membership and sexual preferences.

## Data Protection Principles

Article 5 of the GDPR requires that personal data shall be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard for the purposes for which they are processed, are erased or rectified without delay;
- 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;
- 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.

The GDPR's principle of accountability also requires that the school is able to *demonstrate* that processing is lawful e.g by keeping records and having an audit trail.

## The Lawful Basis for Processing Personal Data

These are set out in Article 6 of the GDPR. At least one of these must apply whenever we process Personal Data:

- **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us, or we are required, to take specific steps before entering into a contract.
- **Legal Obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).
- **Vital Interests:** the processing is necessary to protect someone's life.
- **Public Task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.
- **Legitimate Interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

## The Rights of an Individual

Under GDPR, new provisions have been introduced to develop the protection of personal data and the rights of adults and children. These 8 provisions are:

1. **The right to be informed.** Encompasses our obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how we use personal data. The information we supply about the processing of personal data must be: concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

2. **The right of access.** Individuals have the right of confirmation that their data is being processed, to access their personal data and supplementary information and to be aware of and verify the lawfulness of the processing.
3. **The right of rectification.** The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. If we have disclosed the personal data in question to third parties, we must inform them of the rectification where possible and inform the individuals about the third parties to whom the data has been disclosed.
4. **The right to erasure.** The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:
  - Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
  - When the individual withdraws consent.
  - When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
  - The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
  - The personal data has to be erased in order to comply with a legal obligation.
  - The personal data is processed in relation to the offer of information society services to a child.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
  - To comply with a legal obligation for the performance of a public interest task or exercise of official authority.
  - For public health purposes in the public interest;
  - Archiving purposes in the public interest, scientific research, historical research or statistical purposes; or
  - The exercise or defence of legal claims.
5. **The right to restrict processing.** Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, we are permitted to store the personal data, but not further process it. We can retain just enough information about the individual to ensure that the restriction is respected in future.
  6. **The right to data portability.** This only applies to personal data an individual has provided to us where the processing is based on the individual's consent, or for the performance of a contract, and when processing is carried out by automated means. We must provide that personal data free of charge and in a structured, commonly used and machine readable format.
  7. **The right to object.** Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest, direct marketing (including profiling) and processing for purposes of scientific/historical research and statistics. We must stop processing the personal data unless we can demonstrate compelling legitimate grounds for the processing, which override the

interests, rights and freedoms of the individual or the processing is for the establishment, exercise or defence of legal claims.

8. **Rights in automated decision-making and profiling.** Individuals have the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the individual.

## SAFEGUARDING

GDPR does not prevent, or limit, the sharing of information for the purposes of keeping children safe. Legal and secure information sharing between schools, Children's Social Care, and other local agencies is essential for keeping children safe and ensuring they get the support they need. Information can be shared without consent if to gain consent would place a child at risk. Fears about sharing information must not be allowed to stand in the way of promoting the welfare and protecting the safety of children. As with all data sharing, appropriate organisational and technical safeguards should still be in place.

## OUR DATA PROCESSING PRINCIPLES

### Data Compliance Log

Under GDPR it is not enough to be compliant with the regulations, we must be able to provide demonstrable evidence of our compliance activity.

To that end the DPL will maintain a record of all activities and measures that relate to data protection. All staff are to inform the DPL of such activities and measures so that the record can remain extant.

### Data Audit and Data Subjects

A Data Audit has been conducted to identify what personal data we currently process and how we process it. The audit identified the following categories of Data Subjects:

- **Employment Candidates.** An individual who has applied for employment at Clayesmore, whether or not that application was successful.
- **Current Staff Members.** Anyone directly employed by the school or on the Single Central Register as a volunteer.
- **Former Staff Members.** Anyone who was, but is no longer, employed directly by the school or was on the Single Central Register as a volunteer.
- **Consultants/Contractors.** Anyone providing services to the school who is not directly employed by the school (whether or not on the Single Central Register).
- **Prospective Pupils.** Children who are the subject of an application for a school place or have expressed an interest in doing so.
- **Current Pupils.** Any student on the Prep or Senior school student rolls.
- **Alumni.** Any former pupil of Clayesmore.
- **Prospective Parents.** Individuals with parental responsibility who have applied for a school place for a child or have expressed an interest in doing so.
- **Current Parents.** The parents or guardians of any student on the Prep or Senior school student rolls.
- **Former Parents.** The parents or guardians of a former pupil.
- **Members of the Public.** Anyone who does not fall into one of the other categories.

## USE OF PERSONAL DATA FOR MARKETING AND DEVELOPMENT

### Electronic Marketing

When carrying out electronic marketing the Privacy and Electronic Communications Regulations (PECR) apply, and not GDPR. We can send marketing email or texts to existing 'customers', without obtaining specific consent (called a soft opt-in), if:

- We obtained the contact details of the individual through a 'sale' of a school place or other service to that individual, or negotiations for a school place were entered into but no 'sale' resulted;
- We are only marketing our own similar products or services;
- We have given the person a simple opportunity to refuse or opt out of marketing (during first and every subsequent contact).

With new 'customers' the soft opt-in does not apply and specific consent must be obtained.

### Postal Marketing

If we wish to engage in postal marketing then the GDPR applies. The GDPR specifically says that direct marketing may be regarded as a 'legitimate interest' but it should not be taken for granted and must be used carefully at all times, including flagging up very clearly that the data subject has the right to opt out at any time.

### Obtaining Consent for Using Images

- Consent must be obtained for the use of images of adults or children for marketing purposes. Any consent must be obtained in advance and have a clear Data Protection Policy included with the consent form.
- If we obtained consent to use a photo whilst the child was at school it is reasonable only to use it for the length of time the child attends school, unless it was made clear when the original consent was obtained that we would continue to use it once the child had left school. This does not mean we need to remove all images of former pupils, just that we should not use them in any new material without consent.
- When offering an online service directly to a child, only children aged 13 or over are able to provide their own consent; for younger children, parental consent is required. Children have the same rights as adults over their personal data. When obtaining consent from a child, the Privacy Notice must be written in language the child can easily understand.
- Gaining consent for processing other personal data (e.g. images) the age 13 year rule is probably a reasonable point at which the right to provide consent switches from parent to child. The GDPR talks about a child being 'mature enough' and there is flexibility for national interpretations of when that might be.

## PERSONAL DATA IN A HARD COPY FORMAT

The GDPR does apply to paper records. However, although the GDPR was intended to be 'technologically neutral' the regulation does only apply in two situations:

1. Where processing of personal data is conducted by 'automated means', and

2. Where processing of personal data is not conducted by automated means, but the data “form[s] part of a filing system or [is] intended to be for part of a filing system.”

The first situation involving automated processing is typically interpreted as referring only to situations in which records are stored electronically.

It is difficult to think of a situation in which the processing of paper records is ‘automated’ unless the records are in the process of being converted into a digital format.

The second situation may apply to ‘information kept on paper’ if the paper records are kept within a ‘filing system’. The term ‘filing system’ is defined as “any structured set of personal data which [is] accessible according to specific criteria, whether centralised, decentralised or dispersed . . .” As a result, any files that “are not structured according to specific criteria” do not fall within the scope of the regulation.

The net result is that when paper records are unorganised (e.g., loose documents on a printer, papers on a desk, etc) they are arguably not governed by the GDPR because they are neither structured nor accessible to be easily searched. Conversely, when paper records are organised within a filing system that allows a person to search for specific information or documents there is an argument that they have become ‘structured’ and “accessible according to specific criteria” and thus subject to the GDPR.

## DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The GDPR states that a DPIA should be undertaken whenever there is a change in risk to data subjects. In practice this means that any time we change our systems or processes relating to personal information we should perform a DPIA. A DPIA is a process that systematically describes and assesses the need for, and the proportionality of, the data processing activity. The DPIA must include an assessment of the risks to the rights and freedoms of the data subjects and must also provide measures for addressing those risks and ensuring the protection of the personal data.

The GDPR requires us to document and assess how data and information flows in both hard and digital format throughout our organisation. It requires the data owner to document the data being processed, who receives it, how they process it, where they store it, who it is shared with, how it is shared and the protections that are in place at all stages.

## PRIVACY NOTICES

When we collect personal information we have to provide the Data Subject with certain information in a clear, concise and intelligible manner; clarity of wording is particularly important if the Data Subject is a child. This information we must provide is:

- Identity and contact details of the data controller (or representative) and the Data Protection Lead.
- The purpose of the processing;
- If the legal basis is ‘Legitimate Interests’ then we must explain how.
- If the legal basis is ‘Consent’ then include the right to withdraw consent at any time.
- If the legal basis is a statutory or contractual requirement then the possible consequences of failing to provide the personal data.
- Who will have access to that data and/or who that data will be shared with.



- Any transfers to a country outside of the EEA or Switzerland and the safeguards in place.
- Retention periods or the criteria used to determine a retention period.
- The data subject's rights.
- The additional right to complain to a supervisory authority, in this case the [ICO](#).
- The existence of any automated decision making, including profiling and information about how decisions are made, the significance and the consequences.

## PROCEDURES FOR THE USE OF IMAGES

### General Principles

The use of ordinary and less intrusive images may be covered by the legal basis of 'legitimate interests'. For other specific uses of images of an individual, for example in external marketing, consent should be obtained from the parent or pupil, if not both.

### Using Images of Pupils

There is a lot of misinformation about consent over the use of pupils' photos, but the school does need to take a common sense approach.

GDPR says there needs to be clarity and accountability if we are relying on consent and we need to provide pupils/parents with the following options for the purpose that we would like to use their photographs for:

- Use in and around school, in places that might be seen by visitors,
- On the school website,
- On social media,
- In wider marketing materials used by the school.

We obtain that consent once, and as long as we make it clear to the individual that provides that consent that they can withdraw consent at any time, that is sufficient.

Group and individual portrait photographs will rely on 'soft opt-in' for consent, in that the pupil should be reasonably expected to understand the purposes for which the photo is being taken.

Pupils aged 13 or above (i.e. Senior School) are deemed to be old enough to make their own decisions concerning their own personal data, including images. If consent has been obtained from the parent of a Prep School child, who subsequently moves up to Senior School, then consent for the use of images should be obtained from the child as well. Whether we need to obtain parental consent, in addition to a child aged 13 or more, is not currently clear, but in the interests of diplomacy it may be advisable to seek both.

### Using Images of Staff

In using the images of staff the same principles apply as for pupils. All staff should be asked to provide consent for the 4 options identified in the paragraph above, with a clear understanding that they are able to opt out at any time.

## ‘DASH CAM’ USE

Clayesmore has considered the need for on-board incident capture devices (Dash Cams) and have decided it is required for the protection and safety of persons and property, the prevention or detection of criminal offences, the defence of legal claims, to improve driver training and for use in grievance/disciplinary procedures; it will not be used for other purposes. The decision to use dash cams for these purposes will be reviewed annually by the Data Protection Lead and the Transport Manager.

Clayesmore have installed on-board incident capture devices (Dash Cams) in a number of its vehicles including our minibuses and the school Ford Puma. The operation of the camera system is the responsibility of the Transport Manager. All CCTV (including Dash Cams) at Clayesmore is registered with the Information Commissioner’s Office (ICO).

## CCTV SURVEILLANCE SYSTEMS

Clayesmore has in place a CCTV surveillance system, on the main school site. This system is fully owned by the school and comprises: internal and external fixed position cameras; pan tilt and zoom cameras; monitors; multiplexers; a digital recorder; public information signs. Its installation and operation is in accordance with the CCTV Code of Practice issued by the Information Commissioner’s Office (ICO). The school is also registered as a CCTV operator with the ICO.

The Director of Finance and Operations, being responsible for security, is ultimately responsible for the operation of the system and for ensuring compliance with this policy. However, delegated responsibility for security, including CCTV operations, has been given to the Head of Compliance & Business Support (who also has responsibility as the school’s Data Protection Lead). The CCTV Administration Officer is the Head of ICT. These individuals may be contacted as follows:

Director of Finance and Operations (Nina Bailey Phinn) - [dfo@clayesmore.com](mailto:dfo@clayesmore.com) - 01747 813130

Head of Compliance (Tracy McConnell) - [dpo@clayesmore.com](mailto:dpo@clayesmore.com) - 01747 813255

Head of ICT (James Gater) - [jgater@clayesmore.com](mailto:jgater@clayesmore.com) - 01747 813173

Our use of CCTV surveillance is covered under the Data Protection Act (DPA), the Protection of Freedoms Act (POFA) and the GDPR. Cameras are located at strategic points on the campus, principally at the entrance and exit points of sites and buildings. No camera will be hidden from view and all will be prevented from focussing on the frontages or rear areas of private accommodation. Signs are prominently placed to inform staff, students, visitors and members of the public that a CCTV installation is in use.

The system has been installed with the primary purpose of reducing the threat of crime, protecting premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent.
- Assist in the prevention and detection of crime.
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order.

- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to the EMT and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- Monitor the movement of vehicles on site.
- To provide management information relating to employee compliance with contracts of employment.

With the exception of the Sports Centre, images captured by the system will be monitored and stored in the ICT Department, which remains locked when not occupied. Access to the viewing software requires a personal log-in and as such access is currently restricted to the Head of ICT, the Network Administrator and the HoC; although further remote access may be authorised for the purposes of providing access to live feeds to key staff during a LOCKDOWN. Authority for CCTV investigations can only be made by the Head, the DFO or the Head of Compliance. A record of all 'viewings' is kept, including details of who has viewed images, what was viewed and the reason/authority for viewing.

The Sports Centre CCTV images can be viewed 'live' by the Sports Staff for the purposes of safeguarding. The cameras allow sight of the Fitness Suite and the Reception Foyer for the purposes of ensuring the safety of our pupils and monitoring access to the building.

Images will normally be retained for 28 days before being automatically overwritten. Images will only be kept for longer periods if authorised and for specified purposes. If an individual is recognisable then that becomes personal data and that individual has the same rights over that image as for any other personal data.

## DATA RETENTION REQUIREMENTS

1. The table below contains the ISBA 'suggested' retention periods for various types of data. Except where there is a specific statutory obligation to destroy records, it is misleading to present (or apply) any guidance as if it constitutes prescriptive time 'limits'. Figures given are not intended as a substitute to exercising thought and judgement, or take specific advice, depending on the circumstances.

Type of Record/Document	Suggested Retention Periods
<b>SCHOOL-SPECIFIC RECORDS</b> 1. Registration documents of school 2. Attendance Register 3. Minutes of Governors' meetings 4. Annual curriculum	1. <b>Permanent</b> (or until closure of the school) 2. <b>6 years</b> from the last date of entry, then archive. 3. <b>6 years</b> from date of meeting 4. From end of year: <b>3 years</b> (or <b>1 year</b> for other class records: eg marks / timetables / assignments)

<p><b>INDIVIDUAL PUPIL RECORDS</b></p> <ol style="list-style-type: none"> <li>1. Admissions: application forms, assessments, records of decisions</li> <li>2. Examination results (external or internal)</li> <li>3. Pupil file including: <ol style="list-style-type: none"> <li>a. Pupil reports</li> <li>b. Pupil performance records</li> <li>c. Pupil medical records</li> </ol> </li> <li>4. Special educational needs records (to be risk assessed individually)</li> </ol>	<ol style="list-style-type: none"> <li>1. <b>25 years</b> from date of birth (or, if pupil not admitted, up to 7 years from that decision).</li> <li>2. <b>7 years</b> from pupil leaving school</li> <li>3. ALL: <b>25 years</b> from date of birth (subject, where relevant, to safeguarding considerations: as any material may be relevant to potential claims it should be kept until clear direction is received from the Goddard Enquiry).</li> <li>4. Date of birth plus up to <b>35 years</b> (allowing for special extensions to statutory limitation period)</li> </ol>
<p><b>SAFEGUARDING</b></p> <ol style="list-style-type: none"> <li>1. Policies and procedures</li> <li>2. DBS disclosure certificates (if held)</li> <li>3. Accident / Incident reporting</li> <li>4. Child Protection files</li> </ol>	<ol style="list-style-type: none"> <li>1. Keep a <b>permanent</b> record of historic policies</li> <li>2. No longer than <b>6 months</b> from decision on recruitment, unless DBS specifically consulted – but a record of the checks being made must be kept, if not the certificate itself.</li> <li>3. Keep on record for as long as any living victim may bring a claim (NB civil claim limitation periods can be set aside in cases of abuse). Ideally, files to be reviewed from time to time if resources allow and a suitably qualified person is available.</li> <li>4. <b>Indefinitely.</b></li> </ol>

## DATA BREACHES

A Personal Data breach under the GDPR means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach is much wider than just losing someone's personal data, it is a security incident that has affected the confidentiality, availability or integrity of personal data.

### Dealing with a Data Breach

If a member of staff becomes aware of a personal data breach then it must be reported to the Data Protection Lead (DPL) immediately. Most breaches will be of a low-level nature, where there is no significant risk to the rights and freedoms of individuals, and can be made using the Data Breach Reporting Form. In most cases this will be sufficient, but if the breach has the potential to be high risk to an individual's rights and freedoms then the DPL is to be contacted directly and without delay, followed up by the completion of the Data Breach Reporting Form.

Data Controllers must report breaches to the ICO within 72 hours of becoming aware of it unless the breach is unlikely to result in a risk for individuals. Such a risk would include the potential for identity theft or financial loss. Additionally, if the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must inform those individuals without undue delay.

If a breach is likely to result in a high risk to the rights and freedoms of individuals then we must inform those concerned without undue delay. In notifying individuals we must include in clear and plain language:

- The nature of the personal data breach
- Name and contact details of the Data Protection Lead or other individual acting as a single point of contact
- A description of the likely consequences of the breach
- A description of the measures already taken and being proposed

Although the ICO has the ability to impose fines of a terminal size they are unlikely to do so if we are open and honest and report breaches without undue delay. The ICO is still committed to guiding, advising and educating organisations about how to comply with the regulations. If the ICO can see that we are trying to be compliant then they are unlikely to fine us if we find ourselves with a breach.

## **DEALING WITH A SUBJECT ACCESS REQUEST (SAR) OR A REQUEST TO DELETE, RECTIFY OR TRANSFER PERSONAL DATA**

All Data Subjects have increased rights under the GDPR and as a Data Controller we must respond within one month to any requests to access, delete or rectify the data we hold on them, to restrict how we process their data or to transfer their personal data to a third party. However, this does not necessarily mean that we would automatically agree to any request that came in.

### **Data Subject Access Requests**

Any such requests do not have to be in writing, so staff must be aware of the requirement to pass on any such requests involving the processing of personal data to the Data Protection Officer immediately.

A standard form can be passed to any individual that wishes to make a request involving the processing of their personal data; the use of this form is not mandatory but it does ensure that their request can be dealt with in the most efficient and consistent manner.

Where a DSAR is made electronically, i.e. by email, we are required to respond in a "commonly used electronic form" unless the person making the application requests otherwise. Therefore, the standard format for responding to a DSAR will be PDFs stored on a memory stick and either posted to the individual (using recorded delivery for signature) or handed to the individual personally (a signature for receipt should be obtained). The memory stick (or the files on it) must be password protected and the password should be sent to the subject in a separate message.

Grievances of a third party may not form part of an electronic file, may not be part of a relevant hard copy filing system and should be included in the third party's file rather than the Data Subject, as such it does not have to be disclosed.

ICO guidance on determining whether it is reasonable to disclose information about others is that we need to take into account all of the relevant circumstances, including:

- the type of information that would be disclosed;
- any duty of confidentiality you owe to a third party;
- any steps you have taken to seek consent from the third party;
- whether the third party is capable of giving consent; and
- any express refusal of consent by the third party.

There needs to be a balance between the Data Subject's right of access against the rights of the Third Party. If the third party consents to disclosing information about them, then it would be unreasonable not to do so. However, if there is no such consent, we must decide whether to disclose the information anyway or not. It is a valid choice to not disclose information based on lack of consent or duty of confidentiality.

For any personal data that we process we must have a legal basis for doing so, but unless that legal basis is 'consent' we can decide not to delete, restrict or otherwise change the way we process that data and that we will continue to process that data as we currently do. However, we would need to justify such a decision to the Data Subject and be prepared to justify it to the ICO if the Data Subject were to appeal. The GDPR does contain grounds for refusing such requests, but the default position should be to agree unless we have a very good reason not to.

## DEFINITIONS

**Data Subject:** The individual that the school is holding information about; governors, staff (including volunteers), parents, pupils, contractors and agency workers.

**Personal Data:** Any information that can be used either directly or indirectly to identify a Data Subject. This includes information stored in both digital and 'hard-copy' formats.

**Sensitive Personal Data (also known as 'Special Category Data'):** Information relating to an individual's race or ethnicity, political opinions, religious or philosophical beliefs, physical and mental health, sexual life, criminal convictions or allegations, trade union membership; genetic and biometric data.

**Data Processing:** Any manual or automated activity carried out on personal data, from collection to destruction and everything in between.

**Data Controller:** The school is a Data Controller as we decide why and how personal data will be processed.

**Data Processor:** Any organisation, company or agency that processes personal data on our behalf.

**Data Protection Lead (DPL):** The person nominated by the school to oversee our data protection planning, training and other activities to ensure compliance with GDPR.

**Privacy Policy:** This is where the school sets out how the principles of data protection are applied to all of its personal data processing activities.

**Privacy Statement:** This is more specific than a privacy policy; it's the school's clear and concise public declaration of how the principles of data protection are applied to data processed on our website.

**Data Retention Period:** The length of time that personal data will be kept by the school, or a data processor on instruction from the school. It must be no more than is necessary for the purposes for which the data is collected/processed.

**Explicit Consent:** Active consent in the form of an unambiguous written or spoken statement by the data subject where they have been presented with a clear option to agree or disagree with the processing of their personal data for a specified purpose.

**Subject Access Request:** The method by which a data subject can request all of the personal data relating to them that is held by the school, free of charge.

**Data Audit:** The means of documenting all of the personal data the school processes, the processing it is subjected to and the purposes for which it is processed.

**Pseudonymisation:** The technique of modifying personal data in such a way that it can no longer be associated with the data subject without the addition of other information.