6.19 Data Protection Policy

2025 - 2026

To be read in conjunction with:

6.20 Data and Documentation Retention Policy

6.20.1 Privacy Policy

Data Use and Access Act 2025

Contents

ANNEX Definition of terms

1. Policy statement

1.1 The UK General Data Protection Regulation (UK GDPR) **and the Data Use and Access Act 2025 (DUAA)** ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

1.2 The school will protect and maintain a balance between data protection rights in accordance with the UK GDPR. This policy sets out how we handle the personal data of our pupils, parents, suppliers, employees, workers and other third parties.

1.3 This policy does not form part of any individual's terms and conditions of employment with the school and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy to remain compliant with legal obligations.

1.4 All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

1.5 Everyone has rights regarding the way in which their personal data is handled. During the course of our activities as The Maynard 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.

1.6 We are committed to the protection of all personal data and special category personal data for which we are the data controller.

1.7 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.

1.8 The Maynard School needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements and health and safety for example.

1.9 Agreements to The Maynard School processing personal data is a condition of the acceptance of employment of staff which includes information about previous criminal convictions. It is also necessary to process information so

that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

1.10 Agreement to The Maynard School processing personal data is a condition of the acceptance of students into the school.

1.11 The Maynard School may from time to time, be required to process sensitive personal data. Sensitive personal data includes medical information and data relating to religion, race. Membership of Trade Unions, criminal records and proceedings. The Maynard School has a duty of care to all staff and students and must therefore make sure that employees and those who use the school facilities do not pose a threat or danger to other users.

1.12 Similarly, it may be necessary to process information about a person's criminal convictions, race, gender or family details. This may be to ensure that the school is a safe pace for everyone, or it may be involved with the operation of other policies.

1.13 The Maynard School recognises that, because this information is sensitive, to process could cause concern to individuals; parents/students and staff will therefore be asked to give express written consent for the school to do this.

2 About this policy

2.1 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 UK General Data Protection Regulation ('**UK GDPR**'), the Data Protection Act 2018, the Data Use and Access Act, 2025 and other regulations (together '**Data Protection Legislation**').

2.2 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.

2.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2.4 This policy sets out rules on data protection and the legal conditions that must be satisfied when we process **personal data**.

3 Definition of data protection terms

3.1 All defined terms in this policy are indicated in bold text, and a list of definitions is included in the Annex to this policy.

4 Data Protection Officer

4.1 As an Independent School we are not required to appoint a Data Protection Officer (DPO). However, we have appointed an external organisation as DPO. Their details are as follows: **Data Protection Officer: Judicium Consulting Limited Address: 5th Floor, 98 Theobalds Road, London, WC1X 8WB Email:** dataservices@judicium.com

Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 option 1 then option 1 again

4.2 We have appointed a Data Protection Officer (DPO), who, in conjunction with the DPO is responsible for ensuring compliance with the Data Protection Legislation 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 lynndrake@maynard.co.uk

4.3 The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

5 Data protection principles

5.1 Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:

5.1.1 **processed** fairly and lawfully and transparently in relation to the **data subject**

5.1.2 **processed** for specified, lawful purposes and in a way which is not incompatible with those purposes

5.1.3 adequate, relevant and not excessive for the purpose

5.1.4 accurate and up to date

5.1.5 not kept for any longer than is necessary for the purpose

processed securely using appropriate technical and organisational measures.

5.2 **Personal data** must also:

be **processed** in line with **data subjects'** rights, not be transferred to people or organisations situated in other countries without adequate protection.

5.3 We will comply with these principles in relation to any **processing** of **personal data** by The Maynard School.

6 Fair and lawful processing

6.1 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**.

6.2 For **personal data** to be **processed** fairly, **data subjects** must be made aware:

6.2.1 that the **personal data** is being **processed**

6.2.2 why the **personal data** is being **processed**

6.2.3 what the lawful basis is for that **processing** (see below)

6.2.4 whether the **personal data** will be shared, and if so with whom

6.2.5 the period for which the **personal data** will be held

6.2.6 the existence of the **data subject's** rights in relation to the **processing** of that **personal data**

6.2.7 the right of the **data subject** to raise a complaint with the Information Commissioner's Office in relation to any **processing**.

6.3 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**.

6.4 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:

6.4.1 where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract

6.4.2 where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011)

6.4.3 where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest

6.4.4 where none of the above apply then we will seek the consent of the **data subject** to the **processing** of their **personal data.**

6.5 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:

6.5.1 where the **processing** is necessary for employment law purposes, for example in relation to sickness absence

6.5.2 where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment

6.5.3 where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities

6.5.4 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**.

6.6 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.

6.7 If any **data user** is in doubt as to whether they can use any **personal data** for any purpose then they must contact the DPO before doing so.

Vital Interests

6.8 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 Data Protection Officer in advance, although there may be emergency situations where this does not occur.

Consent

6.9 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.

6.10 There are strict legal requirements in relation to the form of consent that must be obtained from **data subjects**.

6.11 When pupils and or our **workforce** join the Maynard 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.

6.12 In relation to all pupils under the age of 12 years old we will seek consent from an individual with parental responsibility for that pupil.

6.13 We will generally seek consent directly from a pupil who is over the age of 12, 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.

6.14 Pupils will always have the chance to opt out of their image being used.

6.15 If consent is required for any other **processing** of **personal data** of any **data subject** then the form of this consent must:

6.15.1 inform the **data subject** of exactly what we intend to do with their **personal data**

6.15.2 require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in

6.15.3 inform the **data subject** of how they can withdraw their consent.

6.16 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.

6.17 The Data Protection Officer must always be consulted in relation to any consent form before consent is obtained.

6.18 A record must always be kept of any consent, including how it was obtained and when.

7 Processing for limited purposes

7.1 In the course of our activities as The Maynard School, we may collect and **process** the **personal data** set out in our Schedule of 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**).

7.2 We will only **process personal data** for the specific purposes set out in our Schedule of 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.

8 Notifying data subjects

8.1 If we collect **personal data** directly from **data subjects**, we will inform them about:

8.1.1 our identity and contact details as **data controller** and those of the DPO

8.1.2 the purpose or purposes and legal basis for which we intend to **process** that **personal data**

8.1.3 the types of third parties, if any, with which we will share or to which we will disclose that **personal data**

8.1.4 whether the **personal data** will be transferred outside the European Economic Area (**EEA**) and if so the safeguards in place

8.1.5 the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy

8.1.6 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

8.1.7 the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the ICO.

8.2 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.

9 **Adequate, relevant, and non-excessive processing**

9.1 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.

10 **Accurate data**

10.1 We will ensure that **personal data** we hold is accurate and kept up to date.

10.2 We will take reasonable steps to destroy or amend inaccurate or out-of-date data.

10.3 **Data subjects** have a right to have any inaccurate **personal data** rectified. See further below in relation to the exercise of this right.

11 **Timely processing**

11.1 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.

12 **Processing in line with data subject's rights**

12.1 We will **process** all **personal data** in line with **data subjects'** rights, in particular their right to:

12.1.1 request access to any **personal data** we hold about them

12.1.2 object to the **processing** of their **personal data**, including the right to object to direct marketing

12.1.3 have inaccurate or incomplete **personal data** about them rectified

12.1.4 restrict **processing** of their **personal data**

12.1.5 have **personal data** we hold about them erased

12.1.6 have their **personal data** transferred

12.1.7 object to the making of decisions about them by automated means.

The Right of Access to Personal Data

12.2 **Data subjects** may request access to all **personal data** we hold about them. Such requests will be considered in line with the schools Subject Access Request Procedure. Please see Appendix: Subject Access Requests.

If a **data subject** informs the Maynard School that **personal data** held about them by the Maynard School is inaccurate or incomplete, then we will consider that request and provide a response within one month.

12.3 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.

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 Information Commissioner's Office at the time that we inform them of our decision in relation to their request.

13 Data security

13.1 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**.

13.2 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.

13.3 Security procedures include:

13.3.1 **Entry controls.** Any stranger seen in entry-controlled areas should be reported to The Facilities Administrator in the main school office immediately.

13.3.2 **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.) Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access.

13.3.3 **Document printing.** Documents containing **personal data** must be collected immediately from printers and not left on photocopiers.

13.3.4 **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 Information Commissioner's Office guidance on the disposal of IT assets.

13.3.5 **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.

13.3.6 **Working away from the school premises – paper documents.** You must always give serious consideration as to whether it is necessary to take paper records containing personal data or other

confidential information off-site. Paper records should only be taken off-site where there is a **necessity** and not purely for convenience.

There should be a general presumption against taking paper records containing personal or other confidential data off-site and it should only happen when it is absolutely essential to do so and there is no alternative method for accessing or recording the information required, e.g., scanning or accessing online via an encrypted tablet.

If you have determined that it is a **necessity** to take paper records off-site, the following principles must be adopted and followed, to minimise the theft, loss or unauthorised use of personal or other confidential data whilst in transit or off-site.

- Only the minimum amount of data necessary for the job in hand should be removed. Where possible data should be anonymised.

- When in transit from one location to another, records should be transported in a way that mitigates the risks of theft or loss. For example: -

- Do not leave bags or cases containing paper records visible in a car. If it is unavoidable to leave paper records in a car, e.g., whilst filling up with petrol, then lock them in the boot of your card.

- Do not leave paper records unattended in the car for longer than is absolutely necessary, e.g., it would not necessarily be seen to be appropriate to leave paper records in the boot of your car whilst you carry out a large food shop on your way home from work or visit a restaurant or pub before heading home. It would however be viewed as acceptable to leave them locked in the boot of your car whilst collecting a child from nursery or after school care. Paper records should always be secured at home at the end of your workday.

- When travelling on public transport keep the paper records close by at all times. Paper records should not be left in luggage racks or storage areas, as this increases the possibility of theft or of the item being left behind.

- Do not carry paper records ‘loosely’ as this increases the risk of dropping or losing them, use a file or folder to ensure they are secure.

- Paper records should be transported in a separate container to that of any laptop, electronic device or personal effects.

- Whilst off-site, and/or temporarily at home, paper records containing personal or other confidential data that are not being actively worked on must be kept secure and separate from any valuable items such as laptops.

- Paper records taken out of the office should be returned to the place of work as soon as possible. They should not be kept out of

the office for any longer than is necessary to complete the job in hand.

13.3.7 Working away from the school premises – electronic working.

No mobile devices such as laptops, smartphones and tablets can be used to work on at home unless they have been encrypted by the IT Manager.

Under no circumstances can information be downloaded from MIS onto personal devices.

USB Sticks can only be used if they have been encrypted by the IT Manager.

During a pandemic, it may be necessary for staff to work remotely from home, as they did whilst the UK experienced a public health emergency as a result of the COVID-19 pandemic. During such a situation, it is critical that all staff take steps to keep everyone associated with the school safe. Therefore, we need to ensure measures are in place to safeguard the data protection of staff, students and visitors so as not to put them at undue risk. Please see our COVID-19 risk assessment.

13.4 Any member of staff found to be in breach of the above security measures may be subject to disciplinary action. Please refer to our IT Security Policy.

14 Data Protection Impact Assessments

14.1 The Maynard 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.

14.2 In certain circumstances the law requires us to carry out detailed assessments of proposed **processing**. 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 the way that we intend to do so.

14.3 The Maynard School will complete an assessment of any such proposed **processing** and has a template document which ensures that all relevant matters are considered.

14.4 The DPO should always be consulted as to whether a data protection impact assessment is required, and if so how to undertake that assessment.

15 Disclosure and sharing of personal information

15.1 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, Ofsted, ISI, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

15.2 The Maynard 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.

15.3 In some circumstances we will not share safeguarding information. Please refer to our Child Protection Policy.

15.4 Further detail is provided in our Privacy Notice.

16 Data processors

16.1 We contract with various organisations who provide services to the Maynard School including:

The School Photographer for identification purposes

The School's MIS System for trouble shootings purposes only

The School's Bank for the collection of fees by direct debit and the payment of employee's salaries

16.2 In order that these services can be provided effectively we are required to transfer **personal data** of **data subjects** to these **data processors**.

16.3 **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 the Maynard School. The Maynard School will always undertake due diligence of any **data processor** before transferring the **personal data** of **data subjects** to them.

16.4 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**.

17 Images and videos

17.1 Parents and others attending The Maynard School events can take photographs and videos of those events for domestic purposes. For example, parents can take video recordings of a school performance involving their child. The Maynard School does not prohibit this as a matter of policy.

17.2 The Maynard 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 Maynard School to prevent.

17.3 The Maynard 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.

17.4 As a 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.

17.5 Whenever a pupil begins their attendance at the Maynard 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. We will not use images or videos of pupils for any purpose where we do not have consent.

18 Data Protection Complaints

18.1 In line with the Data Use Access Act a parent or pupil who wishes to make a complaint about how their personal information has been used has the facility to do so via our Complaints Policy which has an electronic form for completion by the complainant. Any complaint related to the use of personal information will be acknowledged within 30 days and responded to without undue delay.

19 CCTV

19.1 The Maynard School operates a CCTV system. Please refer to the Maynard School CCTV Policy.

20 Changes to this policy

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

Policy reviewed by LG/LD	September 2025
Next review date	September 2026

Appendix 1 – Subject Access Requests

Under Data Protection Law, Data Subjects have a general right to find out whether the school hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the school are undertaking.

This appendix provides guidance for staff members on how data subject access requests should be handled, and for all individuals on how to make a SAR.

Failure to comply with the right of access under UK GDPR puts both staff and the school at potentially significant risk, and so the school takes compliance with this policy very seriously.

A Data Subject has the right to be informed by the school of the following: -

(a) Confirmation that their data is being processed.
(b) Access to their personal data.
(c) A description of the information that is being processed.
(d) The purpose for which the information is being processed.
(e) The recipients/class of recipients to whom that information is or may be disclosed.
(f) Details of the School's sources of information obtained.
(g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
(h) Other supplementary information.

How to recognise a subject access request

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g., a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the school process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g., during a telephone conversation). The request may refer to the UK GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the school hold about me' will be a data subject access request and should be treated as such.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

How to make a data subject access request

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the school to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

What to do when you receive a data subject access request

All data subject access requests should be immediately directed to DPO who should contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the school must respond to a request and any delay could result in failing to meet those timescales, which could lead to enforcement action by the Information Commissioner's Office (ICO) and/or legal action by the affected individual without delay and failure to do so may result in disciplinary action taken.

Acknowledging the request

When receiving a SAR, the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the school may ask for:

- proof of ID (if needed).
- further clarification about the requested information.
- if it is not clear where the information shall be sent, the school must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The school should work with their DPO in order to create the acknowledgment.

Verifying the identity of a requester or requesting clarification of the request

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The school is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the school may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The school shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the School do not receive this information, they will be unable to comply with the request.

Requests made by third parties or on behalf of children

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a

more general power of attorney. The school may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the school should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the school should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this.
- the nature of the personal data.
- any court orders relating to parental access or responsibility that may apply.
- any duty of confidence owed to the child or young person.
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The school may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

Fee for responding to a SAR

The school will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested. If a request is considered to be manifestly unfounded or unreasonable the school will inform the requester, why this is considered to be the case and that the school will charge a fee for complying with the request.

A fee may also be requested in relation to repeat requests for copies of the same information. In these circumstances a reasonable fee will be charged taking into account the administrative costs of providing the information.

If a fee is requested, the period of responding begins when the fee has been received.

Time Period for Responding to a SAR

The school has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The circumstances where the school is in any reasonable doubt as to the identity of the requester, this period will not commence unless and until sufficient information has been provided by the requester as to their identity, and in the case of a third-party requester, the written authorisation of the data subject has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the school will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

School closure periods

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period. This is because no one will be on site to comply with the request during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e., until a time when we receive the request), however, if we can acknowledge the request, we may still not be able to deal with it until the school re-opens. The school will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

Information to be provided in response to a request

The individual is entitled to receive access to the personal data we process about him or her and the following information:

- the purpose for which we process the data.
- the recipients or categories of recipient to whom the personal data has been or will be disclosed, in particular where those recipients are in third countries or international organisations.
- where possible, the period for which it is envisaged the personal data will be stored, or, if not possible, the criteria used to determine that period.
- the fact that the individual has the right:
    - to request that the Company rectifies, erases or restricts the processing of his personal data; or
    - to object to its processing.
    - to lodge a complaint with the ICO.

- where the personal data has not been collected from the individual, any information available regarding the source of the data.
- any automated decision we have taken about him or her together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly used electronic format.

The information that the school are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The school is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The school is not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the school need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

Depending on the type of information requested, the school may need to search all or some of the following:

- electronic systems, e.g., databases, networked and non-networked computers, servers, customer records, human resources system, email data, back up data, CCTV.
- manual filing systems in which personal data is accessible according to specific criteria, e.g., chronologically ordered sets of manual records containing personal data.
- data systems held externally by our data processors.
- occupational health records.
- pensions data.
- share scheme information.
- insurance benefit information.

The school should search these systems using the individual's name, employee number or other personal identifier as a search determinant.

Requests made by third parties

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request, or it might be a more general power of attorney. The school may also require proof of identity in certain circumstances.

If the School is in any doubt or has any concerns as to providing the personal data of the data subject to the third party, then it should provide the information requested directly to the data subject. It is then a matter for the data subject to decide whether to share this information with any third party.

Requests made on behalf of children

Even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the school should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the school should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this.
- the nature of the personal data.
- any court orders relating to parental access or responsibility that may apply.
- any duty of confidence owed to the child or young person.
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment.
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The school may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

Protection of third parties -exemptions to the right of subject access

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case-by-case basis.

The school will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or
- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individual's consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose.
- any duty of confidentiality they owe to the other individual.
- any steps taken to seek consent from the other individual.
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard, then the DPO should be consulted.

Other exemptions to the right of subject access

In certain circumstances the school may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

Crime detection and prevention: The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

Confidential references: The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual.
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the school receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e., the person giving the reference), which means that the school must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

Legal professional privilege: The School do not have to disclose any personal data which are subject to legal professional privilege.

Management forecasting: The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

Negotiations: The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual were doing so would be likely to prejudice those negotiations.

Refusing to respond to a request

The school can refuse to comply with a request if the request is manifestly unfounded or excessive, taking into account whether the request is repetitive in nature.

If a request is found to be manifestly unfounded or excessive the school can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case the school need to justify the decision and inform the requestor about the decision.

The reasonable fee should be based on the administrative costs of complying with the request. If deciding to charge a fee the school should contact the individual promptly and inform them. The school do not need to comply with the request until the fee has been received.

Record keeping

A record of all subject access requests shall be kept by the DPO. The record shall include the date the SAR was received, the name of the requester, what data the school sent to the requester and the date of the response.

The right to erasure/right to be forgotten

Under Article 17 of the UK GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'.

The right only applies to data held at the time the request is received. It does not apply to data that may be created in the future. The right is not absolute and only applies in certain circumstances.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- the School is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;

- the School is relying on legitimate interests as the basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;

- the School is processing the personal data for direct marketing purposes and the individual objects to that processing;

- the School has processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);

- the School has to do it to comply with a legal obligation; or

- the School has processed the personal data to offer information society services to a child.

How does the right to erasure apply to data collected from children?

There is an emphasis on the right to have personal data erased if the request relates to data collected from children. This reflects the enhanced protection of children's information, especially in online environments, under the UK GDPR.

Therefore, when data is processed that has been collected from children, the School should give particular weight to any request for erasure if the processing of the data is based upon consent given by a child – especially any processing of their personal data on the internet. This is still the case when the data subject is no longer a child, because a child may not have been fully aware of the risks involved in the processing at the time of consent.

Does the School have to tell other organisations about the erasure of personal data?

The UK GDPR specifies two circumstances where the School should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or

- the personal data has been made public in an online environment (for example on social networks, forums or websites).

If the School has disclosed the personal data to others, it must contact each recipient and inform them of the erasure, unless this proves impossible or involves disproportionate effort. If asked to, the School must also inform the individuals about these recipients.

Do the School have to erase personal data from backup systems?

If a valid erasure request is received and no exemption applies then the School will have to take steps to ensure erasure from backup systems as well as live systems. Those steps will depend on particular circumstances, the retention schedule (particularly in the context of its backups), and the technical mechanisms that are available.

It must be absolutely clear to individuals as to what will happen to their data when their erasure request is fulfilled, including in respect of backup systems.

It may be that the erasure request can be instantly fulfilled in respect of live systems, but that the data will remain within the backup environment for a certain period of time until it is overwritten.

The key issue is to put the backup data 'beyond use', even if it cannot be immediately overwritten. It must be ensured that the data within the backup is not used for any other purpose, i.e. that the backup is simply held on School systems until it is replaced in line with an established schedule. Provided this is the case it may be unlikely that the retention of personal data within the backup would pose a significant risk, although this will be context specific.

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

If required by law to process individuals' personal data, then the right to erasure will not apply.

The UK GDPR also specifies two circumstances where the right to erasure will not apply to special category data:

- if the processing is necessary for public health purposes in the public interest (e.g. protecting against serious cross-border threats to health, or ensuring high standards of quality and safety of health care and of medicinal products or medical devices); or
- if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional).

Appendix 2 - Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

Proof of identity: We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g., bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

Section 1

Please fill in the details of the data subject (i.e., the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title

Surname/Family Name

First Name(s)/ Forename

Date of Birth

Address

Post Code

Phone Number

Email address

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

Personal Information

If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.

Details:

Employment records:

If you are, or have been employed by the school and are seeking personal information in relation to your employment please provide details of your staff number, unit, team, dates of employment etc.

Details:

Section 2

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e., the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title

Surname/ Family Name

First Name(s)/Forenames

Date of Birth

Address

Post Code

Phone Number

I am enclosing the following copies as proof of identity (please tick the relevant box):

- ☐ Birth certificate
- ☐ Driving licence
- ☐ Passport
- ☐ An official letter to my address

What is your relationship to the data subject? (e.g., parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- ☐ Letter of authority
- ☐ Lasting or Enduring Power of Attorney
- ☐ Evidence of parental responsibility
- ☐ Other (give details):

Section 3

Please describe as detailed as possible what data you request access to (e.g., time period, categories of data, information relating to a specific case, paper records, electronic records).

I wish to:

- ☐ Receive the information by post*
- ☐ Receive the information by email
- ☐ Collect the information in person
- ☐ View a copy of the information only
- ☐ Go through the information with a member of staff

*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

Please send your completed form and proof of identity by email to: office@maynard.co.uk

ANNEX - DEFINITIONS

Term	Definition
Data	Information, which is stored electronically, on a computer, or in certain paper-based filing systems.
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.
Personal Data	Any information relating to an identified or identifiable natural person (a data subject); an identifiable 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.
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 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.
Data Processors	Any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.
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.
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.
Workforce	Includes any individual employed by *[School/Trust/Academy]* such as staff and those who volunteer in any capacity including governors [and/or trustees / members/ parent helpers].