ISLEWORTH & SYON SCHOOL
FINIS CORONAT OPUS

KEY POLICY

Data Protection Policy

DRAFTED BY:	JHI	**STATUS:**	Statutory
APPROVED:	10/2024	**GOV. PANEL:**	Full Trustees
ISSUE:	3	**NEXT REVIEW:**	As required

Contents

1. Policy Statement

1.1. Everyone has rights with regard to the way in which their **personal data** is handled. During the course of our activities as an academy trust (Trust"), 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**.

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

1.3. 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.

1.4. All members of our **workforce** must comply with this policy when processing **personal data** on our behalf. Any breach of this policy may result in disciplinary or other action.

1.5. Where members of our **workforce** have a specific responsibility in connection with **Processing**, such as capturing consent, reporting a Personal Data Breach or conducting a Data Protection Impact Assessment as referred to in this Data Protection Policy or otherwise, then they must comply with the related policies and privacy guidelines.

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 retained EU law version of the General Data Protection Regulation ((EU)2016/679) ('UK **GDPR'**), the Data Protection Act 2018 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

A list of definitions is included in Appendix 1 to this policy.

4. Data Protection Officer

4.1. As a Trust, we are required to appoint a Data Protection Officer ("DPO"). Please find below details of the School's Data Protection Officer:

Data Protection Officer: Judicium Consulting Limited
Address: 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0203 326 9174
Lead Contact: Craig Stilwell

4.2. These details are also available on the School website under 'Key Contacts'.

4.3. The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy.

4.4. Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

a) If you are unsure of the lawful basis being relied on by the School to process personal data;
b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
c) If you need to draft privacy notices or fair processing notices;
d) If you are unsure about the retention periods for the personal data being processed [but would refer you to the School's Data Retention & Destruction Policy in the first instance];

e) If you are unsure about what security measures need to be put in place to protect personal data;
f) If there has been a personal data breach [and would refer you to the procedure set out in the School's Data Breach Policy];
g) If you are unsure on what basis to transfer personal data outside the EEA;
h) If you need any assistance dealing with any rights invoked by a data subject;
i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
j) If you plan to undertake any activities involving automated processing or automated decision making;
k) If you need help complying with applicable law when carrying out direct marketing activities;
l) If you need help with any contracts or other areas in relation to sharing personal data with third parties. .

4.5. 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:

- **Processed** fairly and lawfully and transparently in relation to the **data subject**;
- **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- **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 Trust.

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:

- that the personal data is being processed;
- why the personal data is being processed;
- what the lawful basis is for that processing (see below);
- whether the personal data will be shared, and if so with whom;
- the period for which the personal data will be held;
- the existence of the **data subject's** rights in relation to the **processing** of that **personal data**; and
- 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:

- where the **processing** is necessary for the performance of a contract between us and the **data subject**, such as an employment contract;
- where the **processing** is necessary to comply with a legal obligation that we are subject to, (e.g. the Education Act 2011);
- where the law otherwise allows us to **process** the **personal data** or we are carrying out a task in the public interest;
- where we are pursuing legitimate interests, (or these are being pursued by a third party), for purposes where they are not overridden because the **Processing** prejudices the interests or fundamental rights and freedoms of **data subjects;** and
- 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 dat**a under following legal grounds:

- where the **processing** is necessary for employment law purposes, for example in relation to sickness absence;
- where the **processing** is necessary for reasons of substantial public interest, for example for the purposes of equality of opportunity and treatment;
- where the **processing** is necessary for health or social care purposes, for example in relation to pupils with medical conditions or disabilities; and
- 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.

6.8. VITAL INTERESTS

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

6.9. CONSENT

6.9.1. 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.

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

6.9.3. When pupils and or our **Workforce** join the Trust, 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, amongst other things. Where appropriate third parties may also be required to complete a consent form.

6.9.4. In relation to all pupils under the age of 12/13 years old we will seek consent from an individual with parental responsibility for that pupil.

6.9.5. We will generally seek consent directly from a pupil who has reached the age of 12/13, however we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

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

- Inform the **data subject** of exactly what we intend to do with their **personal data**;
- Require them to positively confirm that they consent – we cannot ask them to opt-out rather than opt-in; and
- Inform the **data subject** of how they can withdraw their consent.

6.9.7. 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.

6.9.8. Consent may need to be refreshed where we may need to process the **Personal Data** for a different and incompatible purpose which was not disclosed when the consent was first considered by the **Data Subject**.

6.9.9. The DPO must always be consulted in relation to any consent form before consent is obtained.

6.9.10. 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 a Trust, 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:

- our identity and contact details as **Data Controller** and those of the DPO;
- the purpose or purposes and legal basis for which we intend to **process** that **personal data**;
- the types of third parties, if any, with which we will share or to which we will disclose that **personal data**;
- whether the **personal data** will be transferred outside the United Kingdom and if so the safeguards in place;
- the period for which their **personal data** will be stored, by reference to our Retention and Destruction Policy;
- the existence of any automated decision making in the **processing** of the **personal data** along with the significance and envisaged consequences of the **processing** and the right to object to such decision making; and
- the rights of the **data subject** to object to or limit processing, request information, request deletion of information or lodge a complaint with the 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

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.

11.2. We will maintain retention policies and procedures to ensure **Personal Data** is deleted after an appropriate time, unless a law requires that the data is to be kept for a minimum time.

11.3. We shall seek to comply with the rights exercised by **data subjects** as set out in section 12 below as soon as possible and within legal time limits. However, there may be instances where due to circumstances outside of the Trust's control this may not be possible e.g. where the School or Trust has been closed or is only partially operable. In such circumstances data subjects till be notified and provided details about the reason for the delay and when a response can reasonably be expected.

12. Processing in Line with Data Subjects' Rights

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

- request access to any **personal data** we hold about them;
- object to the **processing** of their **personal data**, including the right to object to direct marketing;
- have inaccurate or incomplete **personal data** about them rectified;
- restrict **processing** of their **personal data**;
- have **personal data** we hold about them erased
- have their **personal data** transferred; and
- object to the making of decisions about them by automated means.

12.2. THE RIGHT OF ACCESS TO PERSONAL DATA

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.

12.3. THE RIGHT TO OBJECT

12.3.1. In certain circumstances **data subjects** may object to us **processing** their **personal data**. This right may be exercised in relation to **processing** that we are undertaking on the basis of a legitimate interest or in pursuit of a statutory function or task carried out in the public interest.

12.3.2. An objection to **processing** does not have to be complied with where the school can demonstrate compelling legitimate grounds which override the rights of the **data subject**.

12.3.3. Such considerations are complex and must always be referred to the DPO upon receipt of the request to exercise this right.

12.3.4. In respect of direct marketing any objection to **processing** must be complied with.

12.3.5. The Trust is not however obliged to comply with a request where the **personal data** is required in relation to any claim or legal proceedings.

12.4. THE RIGHT TO RECTIFICATION

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

12.4.2. 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.

12.4.3. 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.

12.5. THE RIGHT TO RESTRICT PROCESSING

12.5.1. **Data subjects** have a right to "block" or suppress the **processing** of personal data. This means that the Trust can continue to hold the **personal data** but not do anything else with it.

12.5.2. The Trust must restrict the **processing** of **personal data**:

- Where it is in the process of considering a request for **personal data** to be rectified (see above);
- Where the Trust is in the process of considering an objection to processing by a **data subject**;
- Where the **processing** is unlawful but the **data subject** has asked the Trust not to delete the **personal data**; and
- Where the Trust no longer needs the **personal data** but the **data subject** has asked the Trust not to delete the **personal data** because they need it in relation to a legal claim, including any potential claim against the Trust.

12.5.3. If the Trust has shared the relevant **personal data** with any other organisation then we will contact those organisations to inform them of any restriction, unless this proves impossible or involves a disproportionate effort.

12.5.4. The DPO must be consulted in relation to requests under this right.

12.6. THE RIGHT TO BE FORGOTTEN

12.6.1. **Data subjects** have a right to have **personal data** about them held by the Trust erased only in the following circumstances:

- Where the **personal data** is no longer necessary for the purpose for which it was originally collected;
- When a **data subject** withdraws consent – which will apply only where the Trust is relying on the individuals consent to the **processing** in the first place;
- When a **data subject** objects to the **processing** and there is no overriding legitimate interest to continue that **processing** – see above in relation to the right to object;
- Where the **processing** of the **personal data** is otherwise unlawful;
- When it is necessary to erase the personal data to comply with a legal obligation.

12.6.2. The Trust is not required to comply with a request by a **data subject** to erase their **personal data** if the **processing** is taking place:

- To exercise the right of freedom of expression or information;
- To comply with a legal obligation for the performance of a task in the public interest or in accordance with the law;
- For public health purposes in the public interest;
- For archiving purposes in the public interest, research or statistical purposes; or
- In relation to a legal claim.

12.6.3. If the Trust has shared the relevant personal data with any other organisation then we will contact those organisations to inform them of any erasure, unless this proves impossible or involves a disproportionate effort.

12.6.4. The DPO must be consulted in relation to requests under this right.

12.7. RIGHT TO DATA PORTABILITY

12.7.1. In limited circumstances a **data subject** has a right to receive their **personal data** in a machine readable format, and to have this transferred to other organisation.

12.7.2. if such a request is made then the DPO must be consulted.

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 main office and if they are not available the site team.

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.)

13.3.3. **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.

13.3.4. **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.

13.3.5. **Working away from the school premises – paper documents.** Staff should only in exceptional circumstances remove any hard copies of documents that contain personal information from the school site.

13.3.6. **Working away from the school premises – electronic working**.

- Any equipment taken away from the school must be stored securely when not in use.
- If a member of staff is working on personal data, it must be in an area where others cannot access the information or listen into confidential calls etc.
- Staff are not permitted to download any information onto personal or portable devices.

13.3.7. **Document printing** – Staff should all think twice and ask themselves – do they need to print documents that contain personal information. Documents containing **personal data** must be collected immediately from printers and not left in spaces where they could ever be viewed by someone else.

13.4. Any member of staff found to be in breach of the above security measures may be subject to disciplinary action.

14. Data Protection Impact Assessments

14.1. The Trust 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 Trust 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, Education and Skills Funding Agency "ESFA", Ofsted, health authorities and professionals, the Local Authority, examination bodies, other schools, and other organisations where we have a lawful basis for doing so.

15.2. The Trust 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.

16. Data Processors

16.1. We contract with various organisations who provide services to the Trust, including for example:

- The school payroll provider
- School catering team

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 Trust. The Trust 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 Trust events are not allowed to take photographs and videos of those events for domestic purposes. For example, taking video recordings of a school performance involving their child.

17.2. As a Trust 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.

17.3. Whenever a pupil begins their attendance at the Trust 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. Video Surveillance

The Trust operates a CCTV system. Please refer to the Trust CCTV Policy.

19. Biometric Data

19.1. The Trust operates a biometric recognition system for the purposes of:

- payment of payment from the school canteen

19.1.1. Before we are able to obtain the Biometric Data of pupils or the Workforce we are required to give notification and obtain consent for this Special Category Data due to additional requirements for processing such data under the Protection of Freedoms Act 2012.

19.2. For the Workforce, written consent will be obtained at the commencement of their position within the Trust and shall continue to be effective unless an objection in writing to the processing of your Biometric Data is received from the individual.

19.3. For pupils under the age of 18 years, the Trust will notify each parent of that pupil (that the school has the contact details for and is able to contact) prior to them commencing their education at the school of the use of our Biometric Recognition System. The school will then obtain the written consent of one of the pupil's parent before obtaining any Biometric Data.

19.4. In the event that written consent cannot be obtained from a parent, or any parent objects in writing or the pupil objects or refuses to participate in the processing of their Biometric Data, the Trust will not process the pupil's Biometric Data and will provide the following alternative means of accessing the above services:

19.5. If a parent has not given permission then students will need to be able to identify themselves at the point of sale. The name provided will be matched to their most recent photo.

19.6. Further information about this can be found in our Notification of Intention to Process Pupil's Biometric Information and our Privacy Notices.

20. Related Policies and Documents

- Data Breach Policy
- Data Retention & Destruction Policy
- Privacy Notices
- Social Media Policy
- CCTV Policy

21. Changes to This Policy

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

Appendix 1 – Definitions

PERSONAL DATA
Means 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.

SPECIAL CATEGORY DATA
Includes 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, sexual orientation or genetic or Biometric Data.

DATA
Is information which is stored electronically, on a computer, or in certain paper-based filing systems.

DATA SUBJECT
An individual about whom such information is stored is known as the Data Subject. For the purpose of this policy include all living individuals about whom we hold personal data. This includes pupils, our workforce, staff, and other individuals. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal information.

DATA USER
Are those of our workforce (including Trustees 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 PROCESSOR
include any person or organisation that is not a data user that processes personal data on our behalf and on our instructions.

DATA CONTROLLER
Are 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.

PROCESSING
Is 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.

AUTOMATED PROCESSING
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision making. Automatic decision making is when a decision is made which is based solely on automated processing (without human intervention) which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)
DPIAs are a tool used to identify risks in data processing activities with a view to reducing them.

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

CRIMINAL RECORDS INFORMATION
This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

BIOMETRIC DATA
Is information about a person's physical or behavioural characteristics or features that can be used to identify them and is obtained or recorded for the purposes of a biometric recognition system and can include fingerprints, hand shapes, features of the eye or information about a person's voice or handwriting.

BIOMETRIC RECOGNITION SYSTEM
Is a system that operates automatically (electronically) and:

- Obtains or records information about a person's physical or behavioural characteristics or features; and
- Compares or otherwise processes that information with stored information in order to establish or verify the identity of the person or otherwise determine whether they are recognised by the system

WORKFORCE
Includes, any individual employed by Trust such as staff and those who volunteer in any capacity including Trustees / Members / parent helpers.

Appendix 2 – Subject Access Requests (SAR)

INTRODUCTION

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.

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

- Confirmation that their data is being processed;
- Access to their personal data;
- A description of the information that is being processed;
- The purpose for which the information is being processed;
- The recipients/class of recipients to whom that information is or may be disclosed;
- Details of the School's sources of information obtained;
- 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
- 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 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 the Headteacher who should contact Judicium as DPO in order to assist with the request and what is required.

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 licence, 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.

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 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 the School will be closed and no one will be on site to comply with the request and we do not always review emails 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 or 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.

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.

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 individuals' 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 receives 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 where doing so would be likely to prejudice those negotiations.