St Dunstan's EDUCATION GROUP

P14 – Data protection and GDPR

Policy Owner: Chief Operating Officer

ISSR Reference: N/A

Interim review: Michaelmas 2024

Approved: Full governing body Michaelmas 2024

Next Review: Lent 2025

Version Control Information

Reason for Amendment	Role	Date	Main Changes
Annual review	Chief Operating Officer	Michaelmas 2024	Change to become a Group-level policy Use of new template

Contents

1. Introduction & aims

This policy is applicable to staff, pupils, parents / carers and visitors.

The UK General Data Protection Regulation (UK GDPR) 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.

St Dunstan's Education Group ('the Group') aims to 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 / carers, suppliers, employees, workers, customers, contractors and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the Group 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 in order to remain compliant with legal obligations.

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 Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

1. Legislation and definitions

1.1 Legislation

This policy is based on advice from Judicium Education, and informed by the following legislation:

- UK General Data Protection Regulation (UKGDPR), 2018
- Data Protection Act, 2018.

1.2 Definitions

Personal data	Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data, but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual, e.g. a name, email address, location or date of birth, or an opinion about that person's actions or behaviour. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.
Special category data	Previously termed 'sensitive personal data', special category data is similar by definition and refers to data concerning an individual data subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.
Data subject	An individual about whom such information is stored is known as the data subject. It includes, but is not limited to, job applicants, employees, pupils, parents/carers.
Data controller	The organisation storing and controlling such information (i.e. the Group) is referred to as the data controller.
Processing	Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or 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.
Criminal records information	This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

3. Roles and responsibilities

3.1 St Dunstan's Education Group

The Group's governing board has ultimate responsibility for data protection but will delegate day-to-day responsibility to the Head of St Dunstan's Education Group. The governing body has a duty to:

- Ensure an approved Data Protection Policy is in place and reviewed annually
- Monitor the application of the Data Protection Policy, including consideration of annual audits.

3.2 The Head of St Dunstan's Education Group

The Head of St Dunstan's Education Group (the Head of Group) is responsible for:

- Day-to-day management of all data protection matters in accordance with the Data Protection Policy
- Delegating responsibilities to other competent members of staff.

3.3 Chief Operating Officer

The Chief Operating Officer (COO) is responsible for:

- Acting as the representative of the data controller on a day-to-day basis
- Acting as first point of contact for individuals whose data the Group processes
- Overseeing the implementation of the Data Protection Policy
- Coordinating subject access requests made to the Group

- Ensuring that the Data Protection Policy, and associated policies, are reviewed no less than annually
- Ensuring that a training needs analysis is carried out to ensure that all staff fully understand this Data Protection Policy and that relevant staff members are trained in relevant areas
- Reporting on data protection matters to the governing body.

3.4 Data Protection Officer

The Data Protection Officer (DPO), Judicium Education, is responsible for:

- Monitoring compliance with data protection law and developing related policies and procedures
- Conducting an annual audit of each individual school's data protection policies and procedures
- Liaising with the Information Commissioners' Office (ICO) regarding possible data breaches.

3.5 Staff

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Completing data protection and cybersecurity training
- Informing the Group of any changes to their personal data, such as a change of address
- Seeking advice from the COO in the following circumstances:
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with contracts or sharing personal data with third parties.

3.6 Pupils and parents/carers

All pupils and parents/carers are responsible for:

- Informing the Group of any changes to their personal data, such as change of address
- Seeking advice from the COO in the following circumstances:
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether the Group has a lawful basis to use personal data in a particular way
- If there has been a data breach

- If they wish to make a subject access request.

4. The processing of personal data

The Group is responsible for and adheres to the principles relating to the processing of personal data as set out in the UK GDPR. These principles are set out below:

4.1 Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner

The Group only collects, processes and shares personal data fairly and lawfully and for specified purposes. The Group must have a specified purpose for processing personal data and special category data as set out in the UK GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review those purposes whilst processing continues to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

The Group may only process a data subject's **personal data** if one of the following fair processing conditions are met:

- The data subject has given their consent
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter a contract
- To protect the data subject's vital interests
- To meet our legal compliance obligations (other than a contractual obligation)
- To perform a task in the public interest or to carry out official functions as authorised by law
- For the purposes of the Group's legitimate interests, where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

The Group may only process **special category data** if entitled to process personal data (using one of the fair processing conditions above) ***AND*** one of the following conditions are met:

- The data subject has given their explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the Group in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay
- To protect the data subject's vital interests
- To meet our legal compliance obligations (other than a contractual obligation)
- Where the data has been made public by the data subject

- To perform a task in the substantial public interest or to carry out official functions as authorised by law
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Where it is necessary for reasons of public interest in the area of public health
- The processing is necessary for archiving, statistical or research purposes.

The Group identifies and documents the legal grounds being relied upon for each processing activity.

Where the Group relies on **consent** as a fair condition for processing, as set out above, it will adhere to the requirements set out in the UK GDPR. Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon, i.e. more than just mere action is required.

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action agreeing to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the Group will normally seek another legal basis to process that data. However, if explicit consent is required the data subject will be provided with full information in order to provide explicit consent.

The Group will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

4.2 Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes

Personal data will not be processed in any matter that is incompatible with the legitimate purposes. The Group will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

4.3 Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

The Group will only process personal data when our obligations and duties require us to. We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes. When personal data is no longer needed for specified purposes, the Group shall delete or anonymise the data. Please refer to each schools' Data Retention Policy for further guidance.

4.4 Principle 4: Personal data must be accurate and, where necessary, kept up to date

The Group will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the Group.

4.5 Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed

Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The Group will ensure that we adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices. The Data Retention Policy details about how we retain and remove data.

4.6 Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage

To assure the protection of all data being processed, the Group will develop, implement and maintain reasonable safeguard and security measures. This includes using measures such as:

- Encryption
- Pseudonymisation, this is where information that directly or indirectly identifies an individual is replaced with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure)
- Ensuring authorised access, i.e. that only people who have a need to know the personal data are authorised to access it
- Adhering to confidentiality principles

- Ensuring personal data is accurate and suitable for the process for which it is processed.

The Group will follow procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The Group will only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place. Full details on security measures are set out in the individual schools' Information Security Policy.

4.7 Sharing personal data

The Group will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party:

- Has a need to know the information for the purposes of providing the contracted services
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place
- The transfer complies with any applicable cross border transfer restrictions
- A fully executed written contract that contains UK GDPR approved third-party clauses has been obtained.

There may be circumstances where the Group is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the Department of Health and Social Care. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals with an organisation outside of the Group shall be clearly defined within written notifications and details and basis for sharing that data given.

4.8 Transfer of data outside the European Economic Area (EEA)

The UK GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the UK GDPR is not undermined. The Group will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the Group's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

4.9 Transfer of data outside of the UK

The Group may transfer personal information outside the UK and/or to international organisations on the basis that the country, territory or organisation is designated as having an adequate level of protection. Alternatively, the organisation receiving the information has provided adequate safeguards by way of binding corporate rules, Standard Contractual Clauses or compliance with an approved code of conduct.

5.Data subject's rights and requests

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data. The rights data subjects have in relation to how the Group handle their personal data are set out below:

- Where consent is relied upon as a condition of processing, to withdraw consent to processing at any time
- Receive certain information about the Group's processing activities
- Request access to their personal data that we hold
- Prevent our use of their personal data for marketing purposes
- Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data
- Restrict processing in specific circumstances
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest
- Request a copy of an agreement under which personal data is transferred outside of the EEA
- Object to decisions based solely on automated processing
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the supervisory authority
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, the relevant staff member within the Group must verify the identity of the individual making the request.

5.1 Direct marketing

The Group is subject to certain rules and privacy laws when marketing. For example, a data subject's prior consent will be required for electronic direct marketing, for example, by email, text or automated calls. The Group will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The Group will promptly respond to any individual objection to direct marketing.

5.2 Employee obligations

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the Group in the course of their employment or engagement. If so, the Group expects those employees to help meet the Group's data protection obligations to those individuals. Specifically, employees must:

- Only access the personal data that they have authority to access, and only for authorised purposes
- Only allow others to access personal data if they have appropriate authorisation
- Keep personal data secure, for example by complying with rules on access to premises, computer access, password protection and secure file storage and destruction
- Not to remove personal data or devices containing personal data from the premises unless appropriate security measures are in place, such as pseudonymisation, encryption and password protection, to secure the information
- Not to store personal information on local drives.

5.3 Accountability

The Group will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the UK GDPR principles. The Group have taken the following steps to ensure and document UK GDPR compliance:

5.3.1 Data Protection Officer (DPO)

Please find below details of the Group's Data Protection Officer:

Data Protection Officer: Judicium Consulting Ltd
Address: Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email: dataservices@judicium.com
Telephone: 0203 326 9174

The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

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

- If they are unsure of the lawful basis being relied on by the Group to process personal data
- If they need to rely on consent as a fair reason for processing
- If they need to draft privacy notices or fair processing notices
- If they are unsure about the retention periods for the personal data being processed
- If they are unsure about what security measures need to be put in place to protect personal data
- If there has been a personal data breach (and would refer you to the procedure set out in each school's Data Breach Policy)
- If they are unsure on what basis to transfer personal data outside the EEA
- If they need any assistance dealing with any rights invoked by a data subject
- Whenever they 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
- If they plan to undertake any activities involving automated processing or automated decision making
- If they need help complying with applicable law when carrying out direct marketing activities
- If they need help with any contracts or other areas in relation to sharing personal data with third parties.

5.3.2 Personal data breaches

The UK GDPR requires the Group to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If a personal data breach has occurred or suspected to have occurred, individuals must not attempt to investigate the matter themselves. It must be reported to the COO in accordance with the Data Breach Policy.

5.3.3 Transparency and privacy notices

The Group will provide detailed, specific information to data subjects. This information will be provided through the privacy notices (and/or fair processing notices) which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. The privacy notices are tailored to suit the data subject and set out information about how we use their data.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the UK GDPR including the identity of the DPO, the Group's contact details, how and why we will use, process, disclose, protect and retain personal data. This information will be provided within our privacy notices.

When personal data is collected indirectly, for example, from a third party or publicly available source, where appropriate, we will provide the data subject with the above information as soon as possible after receiving the data. The Group will also confirm whether that third party has collected and processed data in accordance with the UK GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'children' under the UK GDPR.

5.3.4 Privacy by design

The Group adopts a privacy by design approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start by taking into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processes.

5.3.5 Data protection impact assessments (DPIAs)

In order to achieve a privacy by design approach, the Group conduct DPIAs for any new technologies or programmes being used by the Group which could affect the processing of personal data. DPIAs are carried out when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies
- For the use of automated processing
- For large scale processing of special category data
- For large-scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used
- An assessment of the necessity and proportionality of the processing in relation to its purpose
- An assessment of the risk to individuals
- The risk mitigation measures in place and demonstration of compliance.

5.3.6 Record keeping

The Group is required to keep full and accurate records of our data processing activities. These records include:

- The name and contact details of the Group and its individual schools
- The name and contact details of the DPO
- Descriptions of the types of personal data used
- Description of the data subjects
- Details of the Group's processing activities and purposes
- Details of any third-party recipients of the personal data
- Where personal data is stored
- Retention periods
- Security measures in place.

5.3.7 Training

The Group will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. This policy will be shared with all staff.

5.3.8 Audit

The Group through its DPO regularly test our data systems and processes in order to assess compliance. These are done through annual individual school data audits in order to review the use of personal data.

6. Automated processing and automated decision making

Generally automated decision making is prohibited when a decision has a legal or similar significant effect on an individual unless:

a) The data subject has given explicit consent
b) The processing is authorised by law
c) The processing is necessary for the performance of or entering into a contract.

If certain types of sensitive data are being processed, then (b) or (c) above will not be allowed unless it is necessary for the substantial public interest, for example fraud prevention.

If a decision is to be based solely on automated processing, then data subjects must be informed of their right to object. This right will be explicitly brought to their attention and presented clearly and separately from other information. Furthermore, suitable measures must be put in place to safeguard the data subject's rights and freedoms and legitimate interests.

The Group will also inform the data subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the data subject the right to request human intervention, express their point of view or challenge the decision.

The Group will carry out a data protection impact assessment before any automated processing or automated decision-making activities are undertaken.

7. Monitoring

This policy will be reviewed by the Chief Operating Officer annually. At every review, the policy will be approved by the Finance & Resources Committee.

8. Links with other policies and documents

This Data Protection Policy links to the following policies and documents:

- CCTV Policy
- Data Breach Policy
- Data Retention Policy
- Electronic Information and Communication Systems Policy
- Information Security Policy
- Information Technology Policy (school-level)
- Photographic consent and image usage form (school-level)
- Privacy notices

Appendix A: Subject access requests

Under Data Protection Law, data subjects have a general right to find out whether the Group 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 Group 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 Group at potentially significant risk, and so the Group takes compliance with this policy very seriously.

A data subject has the right to be informed by the Group 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 Group'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 them, 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
- Other supplementary information.

How to recognise a Subject Access Request (SAR)

A SAR 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 Group 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. 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' would constitute 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 us 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 a data subject access request is received

All data subject access requests must be immediately directed to the COO, who will contact Judicium as DPO in order to assist with the request and what is required. There are limited timescales within which the Group 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.

Acknowledging the request

When receiving a SAR, we 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. We will work the DPO to draft the acknowledgement.

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

- Proof of ID (if needed)
- Further clarification about the requested information
- Address/email address to use when sending the requested information
- Consent (if requesting third party data).

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

Before responding to a SAR, the Group 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. We are 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 Group 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 Group 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. We 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 we do not receive this information, we will be unable to comply with the request.

Requests made by third parties or on behalf of children

The Group needs 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. We may also require proof of identity in certain circumstances.

If we have any doubt or concerns as to providing the personal data of the data subject to the third party, then we will 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.

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 carer, to have access to the child's personal data. Before responding to a SAR for information held about a child, we will consider whether the child is mature enough to understand their rights. If we are confident that the child can understand their rights, then we would 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
- Any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged twelve 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 twelve years of age or older, then provided that we are 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, we will require the written authorisation of the child before responding to the requester or provide the personal data directly to the child. We 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

We 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 we will inform the requester why this is considered to be the case and 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 Group 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.

In circumstances where there 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 Group will 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

Th Group may not be able to respond to requests received during or just before closure periods within the one calendar month response period. This is because the schools will be closed/no one will be on site to comply with the request. 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 individual school re-opens. The Group will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If requests are urgent, they should be made 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 them 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 their personal data
    - 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 them together with meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for them.

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 Group 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 we have one

month in which to respond we are 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.

Therefore, we are allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. We are not allowed to amend or delete data to avoid supplying the data.

How to locate information

The personal data the Group 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, we 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 Group will search these systems using the individual's name, employee number or other personal identifier as a search determinant.

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.

We 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 we 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
- 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 Group disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, then we must decide whether to disclose the information anyway. If there are any concerns in this regard the DPO will be consulted.

Other exemptions to the right of subject access

In certain circumstances we 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: We 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: We 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
    - Provision by the individual of any service

This exemption does not apply to confidential references that the Group 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 we must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

- Legal professional privilege: We do not have to disclose any personal data which is subject to legal professional privilege.
- Management forecasting: We 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: We 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.

Refusing to respond to a request

We 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 we can:

- Request a 'reasonable fee' to deal with the request
- Refuse to deal with the request.

In either case we will 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 we decide that we will charge a fee, we will contact the individual promptly and inform them. We 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 COO. The record shall include the date the SAR was received, the name of the requester, what data was sent to the requester and the date of the response.

Appendix B: 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 ONE

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 Group 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 TWO

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):

SECTON THREE

Please describe as detailed as possible what data you request access, 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:

The Head of administrative Services & Events at St Dunstan's College, or The Head of Operations at Rosemead Preparatory School & Nursery.

Appendix B: Clear desk guidance

Leaving a room

- Remove all sensitive and confidential paperwork from plain sight and lock it in a drawer or filing cabinet. This includes mass storage devices such as USB drives and hard drives, or laptops and iPads.
- Drawers should be locked and keys for accessing drawers or filing cabinets should not be left unattended at or near a desk.
- Devices should be screen locked and locked away.
- Rooms should be locked where possible, particularly if the occupant is the last person to leave the room.

Confidential waste

- All wastepaper which contains sensitive or confidential information must be disposed of by using designated confidential waste bins.
- Under no circumstances should this information be placed in regular wastepaper bins.
- If a department destroys large scale files such as HR records, this must be recorded on the data destruction log.

Computer screens

- Computer workstations must be locked when the desk is unoccupied and completely shut down at the end of the workday.
- Computer / laptop screens must be locked when left unattended.
- Devices such as iPads/laptops/Chromebooks/tablets/USB sticks must be locked away at the end of the day.
- An appropriate passcode/password must be set for all accounts and must not be shared with others.
- Screens in public accessibly offices will have privacy screens to prevent people accidentally viewing information that they are not supposed to see.

Displays

- Passwords must not be left in open areas which are visible to others.
- Sensitive or confidential personal data displayed in classrooms should not be left visible or displayed to unauthorised persons.
- Personal data, including, but not limited, to seating plans and student lists, must be stored in folders or in secure places.
- When sharing screens in class, staff must ensure no personal details are shared on the projector.

- Before displaying any names and photos, the relevant school will ensure that the pupil/parent/carer has provided consent.

Printing

- Any print jobs containing personal information should be sent to a secure print location or be retrieved immediately from a local printer.
- To release printing, users will always use fobs (follow-me printing).

Taking data offsite

- Staff are responsible for the security of the data in their possession and when transporting it off site they must always take steps to keep it secure.
- Paper documents should not be removed from the relevant school without the prior permission of the line manager. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. In particular, the information is not to be transported in transparent bags or unsecured storage containers.
- Paper documents must not be read in public spaces or left unattended in any place where it is at risk, e.g., in car boots, in a luggage rack on public transport.
- Paper documents taken home or printed at home containing personal information, sensitive data and confidential information must not be left where they can be seen, accessed or removed by other occupants.
- Paper documents must be collected from printers as soon as they are produced and not left where they can be casually read.
- The master copy of any data must not be removed from site.
- Paper documents containing personal data must be locked away in suitable facilities, such as secure filing cabinets in the home just as they would be onsite.
- Documents containing confidential personal information must not be pinned to noticeboards where other occupants may be able to view them.
- Paper documents must be disposed of securely by shredding and should not be disposed of with ordinary household waste unless it has been shredded first.

Compliance

- If staff have misplaced any information, they must inform the COO as quickly as possible and treat as a possible data breach.