DANES HILL SCHOOL

Overarching Data Protection Policy

This policy applies to the Prep and Pre-Prep School

Author/Reviewer responsible:	DFS, also the Data Protection Lead	**Date of review:**	February 2025
Reviewed by:	Governing Body	**Date of authorisation:**	22.05.2025
		Date of next review:	February 2026

Contents

1 Purpose

1.1 This document outlines the framework that the School (The Vernon Educational Trust Limited, trading as Danes Hill School) has in place to help ensure compliance with data protection law, including the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA 2018**).

2.1 The school is committed to collecting, handling, and processing information in a lawful, secure and safe way, in accordance with the privacy notices served to parents, pupils and employees.

3.1 To signpost staff to relevant procedures and policies and provide the necessary induction and training to enable staff to perform their duties in relation to data protection and cyber security.

4.1 Any references to staff include all staff working in the School (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, governors, contractors, agency staff, peripatetic staff, placement students and volunteers.

2. Legal Framework and Other Policies

2.1 This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018 (DPA)
- School Standards and Framework Act 1998
- Freedom of Information Act 2000
- Electronic Commerce (EC Directive) Regulations 2002
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2018)
- Protection of Freedoms Act 2012
- DfE (2024) 'Keeping children safe in education 2024'

2.2 This policy also has regard to the following guidance:

- ICO (2022) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- DfE (2024) 'Data protection in schools'
- DfE (2023) Generative artificial intelligence (AI) in education

2.3 This policy operates in conjunction with the following school policies:

- Images Authorisation Policy
- Cyber-security Policy
- CCTV Policy
- Safeguarding and Child Protection Policy

- Information and Records Retention Policy
- Informational Security Policy and IT Acceptable Use Form (for staff and separately for pupils)
- Safe Use of AI Policy
- IT Systems Disaster Recovery & Continuity Plan

3. Applicable Data

3.1 For the purpose of this policy, **'personal data'** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded.

3.2 **'Sensitive personal data'** is referred to in the UK GDPR as 'special categories of personal data', and is defined as:

- Biometric data.
- Data concerning health.
- Data concerning a person's sex life.
- Data concerning a person's sexual orientation.
- Personal data which reveals:
    - Political opinions.
    - Religious or philosophical beliefs.
    - Trade union membership.
    - Principles.

3.3 'Sensitive personal data' does not include data about criminal allegations, proceedings or convictions. In the case of criminal offence data, schools are only able to process this if it is either:

- Under the control of official authority; or
- Authorised by domestic law.

3.4 The latter point can only be used if the conditions of the reason for storing and requiring the data fall into one of the conditions below:

- The processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller of the data subject in connection with employment, social security, social protection, health or social care purposes, public health, and research.

3.5 In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered

incompatible with the initial purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.6 The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with" the above principles.

4. Roles, Responsibilities and Governance

4.1 The governors have appointed the Director of Finance and Operations as the Data Protection Lead. The Data Protection Lead (DPL) is responsible for managing the School's compliance with data protection law and may seek support from the Head of Compliance and other external data protection advisors or lawyers. The governors have ensured that the Data Protection Lead has sufficient time and resources to fulfil their tasks. In their absence, staff are required to contact the Head of Compliance or the Operations Director.

4.2 The Data Protection Lead regularly reports to the School's governors who are responsible for the School's data protection compliance. Data protection is a standing item on the agenda at People, Governance and Risk Committee (PGR) meetings.

4.3 The People, Governance and Risk Committee (governors committee) has specific responsibility for data protection.

4.4 Governors are required to oversee a culture of information governance which values, protects and uses information for the benefit of the school, pupils, staff and the wider community.

4.5 All staff have a role to play in our data protection compliance. Staff must follow applicable policies and make sure they are aware of information governance requirements set out in their job or role description. Staff are encouraged to ask questions and raise concerns with the Data Protection Lead or their line manager. This allows us to regularly review and strengthen the data protection measures that we have in place.

5. Training

5.1 All staff receive data protection training as part of their induction and refresher training is

provided annually. The training is a mixture of face to face training delivered during the inset programme by the Data Protection Lead and online training and staff must pass a test to complete the training.

5.2 The training includes (but is not limited to) the practical application of the UK GDPR's principles in a school context, guidance on how to keep personal data secure and when staff should speak to the Data Protection Lead.

5.3 The Senior Leadership Team and governors receive additional training on an annual basis. This training has been specifically designed for their roles.

5.4 The Data Protection Lead attends external training annually which is appropriate to their role as the senior individual who leads on the School's data protection compliance.

5.5 Other teams and departments are given data protection training which is specific to their role or function as follows: IT, Finance and Marketing & Admissions.

6. Documentation

6.1 Documenting how we comply with data protection law is a key part of our compliance. The School complies with its GDPR duties by:

- maintaining a record of how we use personal data as required under Article 30 of the UK GDPR. The Data Protection Lead is responsible for maintaining this record;
- documenting our lawful bases for using personal data through our privacy notices;
- keeping a record of our legitimate interests assessments;
- carrying out risk assessments and when required a Data Protection Impact Assessment;
- retaining records of any consents obtained to use personal data by recording these on individual pupil records in iSams, the school's MIS tool.
- maintaining a register of any data breaches. The Data Protection Lead is responsible for completing this. All staff understand that they must inform the Data Protection Lead of any suspected breaches so that the register can be kept up to date and the most appropriate action is taken to inform, rectify and report the breach, if appropriate;
- recording when staff complete data protection training to ensure that all staff have received the appropriate level of training; and
- maintaining an appropriate Policy Document regarding our processing of special category personal data and criminal offence data as required by the DPA 2018.

7. Privacy notices

7.1 The School has privacy notices for pupils, parents and employees, which are published on the School's website.

7.2 We are mindful that some of our pupils are competent to exercise their own data protection rights. In light of this, we have developed a privacy notice for pupils which is age appropriate and addressed directly to the pupils.

7.3 In addition, the School explains how personal data will be used on a case-by-case basis as appropriate. For example, forms that are used to collect personal data will include a brief description of how and why it will be used, and cross refer to the applicable privacy notice.

8. Data protection by design and default

8.1 The School has built the data protection principles into its practices by implementing appropriate technical and organisation measures. This is known as data protection by design.

8.2 We also ensure that we only use the minimum amount of personal data to achieve our purposes - known as data protection by default.

8.3 More specifically we do the following:

8.3.1 at the start of any new project, or new activity, which involves using personal data (e.g. working with a new external activity provider, implementing new software or hardware) the Data Protection Lead considers how we will comply with the data protection principles and if a DPIA is required.

8.3.2 we make it clear on any data collection forms what personal data must be provided and what is optional;

8.3.3 we proactively consider data protection risks and adopt appropriate measures to protect personal data (e.g. encryption, physical security);

8.3.4 our external facing documents (e.g. privacy notices) are accessible and age appropriate;

8.3.5 before we share personal data externally, we check that we have a lawful basis and that the sharing is fair;

8.3.6 we regularly review the measures which are in place to ensure that they are still appropriate;

8.3.7 we have developed a culture where staff understand the importance of data protection; and

8.3.8 if there has been a problem, or a "near miss", we will look at what has happened to improve our practices, for example, by providing additional staff training and awareness.

8.4 The School has various internal written procedures in place to comply with our obligations under the UK GDPR. This includes in relation to:

8.4.1 computer and network security;

8.4.2 the secure destruction of personal data - both electronic and paper copies;

8.4.3 individuals exercising their rights;

8.4.4 ensuring that we only use processors who comply with the UK GDPR; and

8.4.5 physical security when the School site is used by external parties.

8.5 The Data Protection Lead determines whether a Data Protection Impact Assessment is required before the School begins any new type of processing activity. For example, before the School introduces new software to store pupil records.

9. Lawful processing

9.1 The legal basis for processing data will be identified and documented prior to data being processed. Under the UK GDPR, data will be lawfully processed under the following conditions:

9.2 The consent of the data subject has been obtained

9.3 The school will only process personal data without consent where any of the above purposes cannot reasonably be achieved by other, less intrusive means or by processing less data.

- Processing is necessary for a contract held with the individual, or because they have asked the school to take specific steps before entering into a contract
- Processing is necessary for compliance with a legal obligation (not including contractual obligations)
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Processing is necessary for protecting vital interests of a data subject or another person, i.e. to protect someone's life
- Processing is necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject – this condition is not available to processing undertaken by the school in the performance of its tasks

9.4 Sensitive data will only be processed under the following conditions:

- Explicit consent of the data subject
- Processing relates to personal data manifestly made public by the data subject
- Processing is necessary for:
    - Carrying out obligations under employment, social security or social protection law, or a collective agreement
    - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent
    - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity
    - Reasons of substantial public interest with a basis in law which is proportionate to the aim pursued and which contains appropriate safeguards
    - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services with a basis in law
    - Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with a basis in law

9.5 When none of the above apply, consent will be obtained by the data subject to the processing of their special category personal data.

9.6 The school will ensure that it has privacy notices established which clearly outline the reasons why it needs to collect personal data. The privacy notice will include the following explicit details:

- Why the school needs to collect personal data
- What the school plans to do with the personal data
- How long the school will keep the personal data
- Whether the school will share the personal data with any external organisations
- The privacy notice will be clear and accessible to data subjects. The privacy notice will also be reviewed by the school's DPO at least annually and whenever significant changes are made to how the school processes the data that it collects.

9.7 The school will ensure that any parents, pupils and staff whose personal data is included will be notified of any significant changes to the privacy notice or the way in which the school processes the data.

- 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.
- Whether the personal data will be shared, and if so, with whom.
- The existence of the data subject's rights in relation to the processing of that personal data.
- The right of the data subject to raise a complaint with the ICO in relation to any processing.

9.8 The school has privacy notices for the following groups, which outline the information above that is specific to them:

- Staff Privacy Notice
- Pupil Privacy Notice
- Privacy Notice for Parents

9.9 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 may include medical emergencies where it is not possible for the data subject to give consent to the processing. In such circumstances, the DPO will be consulted and a decision made only after seeking further clarification.

9.10 Where the school relies on:

- 'Performance of contract' to process a child's data, the school considers the child's competence to understand what they are agreeing to, and to enter into a contract.
- 'Legitimate interests' to process a child's data, the school takes responsibility for identifying the risks and consequences of the processing, and puts age-appropriate safeguards in place.

- Consent to process a child's data, the school ensures that the requirements outlined in the 'Consent' section are met.

10. Consent

10.1 Consent must be a positive indication expressly confirmed in words. It cannot be inferred from silence, inactivity, a positive action without words or pre-ticked boxes. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes. Consent can be withdrawn by the individual at any time.

10.2 Where consent is given, a record will be kept documenting how and when consent was given, and what the data subject was told.

10.3 The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained.

10.4 When pupils and staff join the school, the staff member or pupil (or, where appropriate, pupil's parent) will be required to complete a consent form for personal data use. This consent form deals with the taking and use of photographs and videos, amongst other things. Where appropriate, third parties may also be required to compete a consent form.

10.5 Where the school opts to provide an online service directly to a child, the child is aged 13 or over, and the consent meets the requirements outlined above, the school obtains consent directly from that child; otherwise, consent is obtained from whoever holds parental responsibility for the child, except where the processing is related to preventative or counselling services offered directly to children. In all other instances with regards to obtaining consent, an appropriate age of consent is considered by the school on a case-by-case basis, taking into account the requirements outlined above

11.Individuals' rights

11.1 We are committed to allowing individuals to exercise their rights under the UK GDPR. Theserights are as follows:

A. Right to be informed

Adults and children have the same right to be informed about how the school uses their data. The privacy notices supplied to individuals, including children, in regard to the processing of their personal data will be written in clear, plain, age-appropriate language which is concise, transparent, easily accessible and free of charge.

In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller, the controller's representative, where applicable, and the DPL
- The purpose of, and the lawful basis for, processing the data
- The legitimate interests of the controller or third party
- Any recipient or categories of recipients of the personal data
- Details of transfers to third countries and the safeguards in place

- The retention period of criteria used to determine the retention period
- The existence of the data subject's rights, including the right to:
- Withdraw consent at any time
- How to lodge a complaint with a supervisory authority
- The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences

B. **Right of access** (i.e. making a subject access request);

Individuals, including children, have the right to obtain a copy of their personal data as well as other supplementary information, including confirmation that their data is being processed, and the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied.

- A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual requests further copies of the same information. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.
- Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.
- Where a SAR has been made for information held about a child, the school will evaluate whether the child is capable of fully understanding their rights. If the school determines the child can understand their rights, it will respond directly to the child.
- All requests will be responded to without delay and at the latest, within **one month** of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.
- Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.
- The school will ensure that information released in response to a SAR does not disclose personal data of another individual. If responding to the SAR in the usual way would disclose such data, the school will:
    - Omit certain elements from the response if another individual's personal data would be disclosed otherwise.
    - Reject requests that cannot be fulfilled without disclosing another individual's personal data, unless that individual consents, or it is reasonable to comply without consent.
    - Explain to the individual who made the SAR why their request could not be responded to in full.
- In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to – the time limit for responding to the request will be paused until clarification from the individual is received

C. Right to rectification

Individuals, including children, are entitled to have any inaccurate or incomplete personal data rectified.

Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

Requests for rectification will be investigated and resolved, where appropriate, free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that it considers to be manifestly unfounded or excessive or if an individual makes multiple requests at once. The school reserves the right to refuse to process requests for rectification if the School considers they are manifestly unfounded or excessive or if exemptions apply.

The school will take reasonable steps to ensure that data is accurate or is rectified if inaccurate, implementing a proportional response for data that has a significant impact on the individual, e.g. if significant decisions are made using that data. The school will restrict processing of the data in question whilst its accuracy is being verified, where possible.

Where the personal data in question has been disclosed to third parties, the school will inform them of the rectification where possible. Where appropriate, the school will inform the individual about the third parties that the data has been disclosed to.

Where no action is being taken in response to a request for rectification, or where the request has been investigated and the data has been found to be accurate, the school will explain the reason for this to the individual, and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

D. Right to erasure

Individuals, including children, hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing. Individuals, including children, have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected or processed
- When the individual withdraws their consent where consent was the lawful basis on which the processing of the data relied
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child
- The school will comply with the request for erasure without undue delay and at the latest within one month of receipt of the request.

The school has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest

- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The establishment, exercise or defence of legal claims.

The school has the right to refuse a request for erasure for special category data where processing is necessary for:

- Public health purposes in the public interest, e.g. protecting against serious cross-border threats to health.
- Purposes of preventative or occupational medicine, the working capacity of an employee, medical diagnosis, the provision of health or social care, or the management of health or social care systems or services.

Requests for erasure will be handled free of charge; however, the school may impose a 'reasonable fee' to cover the administrative costs of complying with requests that are manifestly unfounded or excessive or if an individual makes multiple requests at once.

As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so. Where personal data has been made public within an online environment, the school will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

E. **Right to restriction**

Individuals, including children, have the right to block or suppress the school's processing of personal data.

The school will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the school has verified the accuracy of the data
- Where an individual has objected to the processing and the school is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the school no longer needs the personal data, but the individual requires the data to establish, exercise or defend a legal claim.

In the event that processing is restricted, the school will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future. The school will inform individuals when a restriction on processing has been lifted.

Where the school is restricting the processing of personal data in response to a request, it will make that data inaccessible to others, where possible, e.g. by temporarily moving the data to another processing system or unpublishing published data from a website.

If the personal data in question has been disclosed to third parties, the school will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

The school reserves the right to refuse requests for restricting processing if theSchool considers they are manifestly unfounded or excessive or if exemptions apply. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

F. Right to data portability

Individuals, including children, have the right to obtain and reuse their personal data for their own purposes across different services. The right to data portability only applies in the following cases:

Where personal data has been provided directly by an individual to a controller

Where the processing is based on the individual's consent or for the performance of a contract

When processing is carried out by automated means:

- Personal data can be easily moved, copied or transferred from one ICT environment to another in a safe and secure manner, without hindrance to usability. Personal data will be provided in a structured, commonly used and machine-readable form. Where feasible, data will be transmitted directly to another organisation at the request of the individual. The school will not be required to adopt or maintain processing systems which are technically compatible with other organisations.

The school will provide the information free of charge.

In the event that the personal data concerns more than one individual, the school will consider whether providing the information would prejudice the rights of any other individual.

The school will respond to any requests for portability within one month. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

Where no action is being taken in response to a request, the school will, without delay and within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

G. Right to object

The school will inform individuals, including children, of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information. Individuals, including children, have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Processing used for direct marketing purposes
- Processing for purposes of scientific or historical research and statistics.
- Where personal data is processed for the performance of a legal task or legitimate interests:
- An individual's grounds for objecting must relate to his or her particular situation.
- The school will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate

compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

The school will respond to objections proportionally, granting more weight to an individual's objection if the processing of their data is causing them substantial damage or distress.

Where personal data is processed for direct marketing purposes:

- The right to object is absolute and the school will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The school cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.
- The school will retain only enough information about the individual to ensure that the individual's preference not to receive direct marketing is respected in future.
- Where personal data is processed for research purposes:
- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the school is not required to comply with an objection to the processing of the data.
- Where the processing activity is outlined above, but is carried out online, the school will offer a method for individuals to object online.
- The DPO will ensure that details are recorded for all objections received, including those made by telephone or in person, and will clarify each objection with the individual making the request to avoid later disputes or misunderstandings. The school will respond to all objections without undue delay and within one month of receiving the objection; this may be extended by a further two months if the request is complex or repetitive.
- Where no action is being taken in response to an objection, the school will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

H. Rights in relation to automated decision-making and profiling.

Staff are trained to recognise when an individual is exercising a right under the UK GDPR and to pass this immediately to the Data Protection Lead.

The School keeps a log of all requests to exercise rights with the applicable deadline for our response. This log is maintained by the Data Protection Lead.

To ensure that we meet our obligations the Data Protection Lead co-ordinates our response to all requests. The Data Protection Lead has detailed knowledge of how to respond to individuals' rights and has received external training. The Data Protection Lead will involve other members of staff, as appropriate, in formulating the School's response.

Consideration is given to at least the following issues when responding to rights requests:

- the importance of responding within the statutory timeframe, usually one calendarmonth (but this can be extended by up to two months for complex requests);
- whether a pupil's consent should be sought before responding to their parent orguardian;
- whether further engagement with the requester is needed, e.g. to ask for ID or toseek clarification of their request;

- the exemptions under the DPA 2018;
- the provision of supplementary information (e.g. sources and purposes) under asubject access request;
- whether the request can be refused, or a reasonable fee charged, because it ismanifestly unfounded or excessive; and
- how to securely send our response to the requester.

12.Information security

12.1 The School has put in place technical and organisational measures to ensure the confidentiality, availability and integrity of personal data. The Data Protection Lead is responsible for determining the appropriate organisational measures, for example, staff training and guidance**.**

12.2 The IT manager leads on the technical side of our information security, for example, network security. The School follows guidance from the National Cyber Security Centre and keeps up to date with the latest cyber security news and alerts.

12.3 The School has implemented an Information Security Policy for staff.

12.4 We appreciate that prompt action is vital when handling information security incidents. Staff are trained to report any suspicions or concerns regarding potential personal data breaches to the Data Protection Lead immediately.

12.5 The Data Protection Lead will carry out an initial investigation and determine if the incident constitutes a personal data breach.

13.Data Breaches

13.1 The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The DPL will ensure that all staff are made aware of, and understand, what constitutes a data breach as part of their training.

13.2 Effective and robust breach detection, investigation and internal reporting procedures are in place at the school, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

13.3 Where the school faces a data security incident, the DPO will coordinate an effort to establish whether a personal data breach has occurred, assess the significance of any breach, and take prompt and appropriate steps to address it.

13.4 All notifiable breaches will be reported to the Information Commissioner's Office (ICO) within 72 hours of the school becoming aware of them. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the data subjects concerned will be contacted directly. The risk of the breach having a detrimental effect on the individual, and the need to notify the ICO, will be assessed on a case-by-case basis. Within a breach notification to the supervisory authority, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of

individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects

13.5 Where notifying an individual about a breach to their personal data, the school will provide specific and clear advice to individuals on the steps they can take to protect themselves and their data, where possible and appropriate to do so.

13.6 The school will ensure all facts regarding the breach, the effects of the breach and any decision-making processes and actions taken are documented in line with the UK GDPR accountability principle and in accordance with the Records Management Policy.

13.7 Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself. The school will work to identify the cause of the breach and assess how a recurrence can be prevented, e.g. by mandating data protection refresher training where the breach was a result of human error.

14 **Safeguarding**

14.1 The school understands that the UK GDPR does not prevent or limit the sharing of information for the purposes of keeping children safe.

14.2 The school will ensure that staff have due regard to their ability to share personal information for safeguarding purposes, and that fears about sharing information must not be allowed to obstruct the need to safeguard and protect pupils. The governing board will ensure that staff are:

- Confident of the processing conditions which allow them to store and share information for safeguarding purposes, including information, which is sensitive and personal, and should be treated as 'special category personal data'.

- Aware that information can be shared without consent where there is good reason to do so, and the sharing of information will enhance the safeguarding of a pupil in a timely manner.

14.3 The school will ensure that information pertinent to identify, assess and respond to risks or concerns about the safety of a child is shared with the relevant individuals or agencies proactively and as soon as is reasonably possible. Where there is doubt over whether safeguarding information is to be shared, especially with other agencies, the DSL will ensure that they record the following information:

- Whether data was shared
- What data was shared
- With whom data was shared
- For what reason data was shared
- Where a decision has been made not to seek consent from the data subject or their parent
- The reason that consent has not been sought, where appropriate

- The school will aim to gain consent to share information where appropriate; however, staff will not endeavour to gain consent if to do so would place a child at risk. The school will manage all instances of data sharing for the purposes of keeping a child safe in line with the Child Protection and Safeguarding Policy.

14.4 Pupils' personal data will not be provided where the serious harm test is met. Where there is doubt, the school will seek independent legal advice.

15 **Processors**

15.1 The School has procedures in place to check that the organisations acting as our processors are complying with the UK GDPR. The Data Protection Lead and IT manager are responsible for implementing these procedures.

15.2 The School has contracts in place with our processors which include the specific terms required by the UK GDPR. Legal advice is sought as required regarding these contracts.

15.3 Staff are trained to speak to the Data Protection Lead if they need to share information with an organisation which may act as the School's processor so that the Data Protection can check that the appropriate measures are in place.

16 **Cloud computing**

16.1 For the purposes of this policy, 'cloud computing' refers to storing and accessing data and programs, such as documents, photos or videos, over the internet, rather than on a device's hard drive. Cloud computing involves the school accessing a shared pool of ICT services remotely via a private network or the internet.

16.2 All staff will be made aware of data protection requirements and how these are impacted by the storing of data in the cloud, including that cloud usage does not prevent data subjects from exercising their data protection rights.

16.3 If the cloud service offers an authentication process, each user will have their own account. A system will be implemented to allow user accounts to be created, updated, suspended and deleted, and for credentials to be reset if they are forgotten, lost or stolen. Access for employees will be removed when they leave the school.

16.4 As with files on school devices, only authorised parties will be able to access files on the cloud. An audit process will be put in place to alert the school should unauthorised access, deletion or modification occur, and ensure ongoing compliance with the school's policies for the use of cloud computing.

17 **Data retention**

17.1 The Information and Records Retention Policy sets the approach to storing, reviewing and destroying of records. Data will not be kept for longer than is necessary. Unrequired data will be deleted as soon as practicable. Some educational records relating to former pupils or employees of the school may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts. Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

18 **Use of Artificial Intelligence (AI)**

18.1 The Safe Use of AI policy sets the procedure for the use of artificial intelligence in school.

18.2 At Danes Hill, recognise that the use of artificial intelligence (AI) can help to positively affect teacher workload, develop pupils' intellectual capabilities and prepare them for how emerging technologies will change workplaces. While there are many benefits to the use of AI tools, the content they produce may not always be accurate, safe or appropriate, and could lead to malpractice.

18.3 The School aims to ensure that AI is used effectively, safely and appropriately to deliver excellent education that prepares our pupils to contribute to society and the future workplace

19. International Transfers

19.1 The School maintains a record of when it transfers personal data outside of the UK and what adequacy decision, safeguard or derogation is relied on under the UK GDPR. The Data Protection Lead is responsible for maintaining this record.

19.2 Staff are trained to speak to the Data Protection Lead before transferring personal data outside of the UK.

20. Data Protection Fee

20.1 The School has procedures in place to ensure that the data protection fee is paid to the Information Commissioner's Office for all controllers connected to the School.

20.2 The Data Protection Lead is responsible for ensuring the fee is paid on time.