DANESHILL SCHOOL

DATA PROTECTION POLICY

This policy applies to all parts of Daneshill School including The Early Years Foundation Stage.

Created: May 2018
Reviewed: Sept 2022
Next review date: Sept 2023

INDEX

1. AIMS

Daneshill School aims to ensure that all personal data collected about staff, pupils, parents, advisors, contractors, volunteers, visitors and other individuals is collected, stored and processed in accordance with current data protection legislation. This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. LEGISLATION AND GUIDANCE

The policy meets the requirements of the GDPR and the expected provisions of the Data Protection Bill. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

3. DEFINITIONS

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. For example: • Name (including initials) Home address, contact details • Pupil records • Photos and videos Personal data may exist as an electronic record and as a hard copy (paper or otherwise)
Special Categories of Personal Data	Personal data which is more sensitive and so needs more protection. For example: • Religious beliefs • Medical history • Special Educational Needs
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying and sharing. Processing can be automated or manual.
Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data Processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.

Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.
Third Party	Any external organization with whom personal data is shared.

4. THE DATA CONTROLLER

The School processes personal data relating to parents, pupils, staff, contractors, volunteers, visitors and others, and therefore is a Data Controller. The Bursar has responsibility as the Data Protection Officer on behalf of the School.

5. ROLES AND RESPONSIBILITIES

This policy applies to all staff employed by the School, and to external organisations or individuals working on our behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Proprietor

The Proprietor has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

5.2 Primary Data Controller

The Data Protection Officer is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. The Bursar fulfils this responsibility on a day-to-day basis.

5.3 All Staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy.
- Informing the School of any changes to their personal data, such as change of address.
- Contacting the Data Protection Officer in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure.
    - 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 wish to share personal data with third parties
    - 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.

6. DATA PROTECTION PRINCIPLES

The School seeks to address (amongst other things) the following key regulatory principles within this policy:

- **Lawfulness, fairness and transparency** in the handling and use of personal data. The School will ensure that we make it clear how we are using personal data, on which "lawful bases" we are processing the information and that we recognise and uphold the rights of the Data Subjects.

- **Limiting the processing of personal data to specified, explicit, and legitimate purposes**. The School shall not use personal data for purposes that are "incompatible" with the purpose for which the data was originally collected.

- **Minimising the collection and storage of personal data** so that we only collect and retain what we need to for the intended purpose of processing.

- **Ensuring the accuracy** of personal data and enabling it to be erased or rectified without delay.

- **Limiting the storage of personal data**. The School will ensure that we retain personal data only as long as necessary to achieve the purposes for which it was collected.

- **Ensuring security, integrity, and confidentiality of personal data**. The School employs appropriate technical and organisational security measures to keep personal data secure.

7. COLLECTING PERSONAL DATA

7.1 Processing

The School processes information in order to fulfil our contractual obligations to provide educational services, safeguard and promote the welfare of its pupils, promote the objects and interests of the School, facilitate the efficient operation of the School and ensure that all relevant legal obligations of the School are complied with.

The School may process different types of information about staff, pupils, parents, governors, contractors, volunteers, visitors and other individuals for the purposes set out above. That information may include (but is not limited to):

- Personal details such as home address, contact details, date of birth and next of kin
- Identification documents
- Pupils' performance at School, including assessments, reports, examination reports, discipline record, attendance information
- Special educational needs
- Medical records and information, including details of any illnesses, allergies or other medical conditions suffered by a child
- Safeguarding information
- Details of any support received, including learning support, therapists, counselling, care

plans and support providers
- Sensitive personal data such as ethnic group, religious beliefs
- Images of pupils and staff (and occasionally other individuals) engaging in School activities
- Bank details and National Insurance Number
- Performance Development Records

7.2 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

The data needs to be processed so that the School can **fulfil a contract** with the individual, or to enter into a contract

- The data needs to be processed so that the School can **comply with a legal obligation**

- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life

- The data needs to be processed for the **legitimate interests** of the School or a third party (provided the individual's rights and freedoms are not overridden)

- The individual (or their parent/guardian when appropriate in the case of a pupil) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Bill.

Whenever we initially collect personal data directly from individuals, we will provide them with the relevant information required by data protection law in the form of a Privacy Notice.

Personal data (including sensitive personal data, where appropriate) is processed by the School in order to:

- administer admissions
- support pupils' teaching and learning;
- monitor and report on pupil progress;
- provide appropriate pastoral care and safeguarding
- communicate with individuals with links to the School
- where appropriate, promote the School to prospective pupils (including through the School's prospectus, website and social media applications);
- other reasonable purposes relating to the operation of the School including to obtain appropriate professional advice and insurance for the School.
- Process payroll
- Facilitate safe recruitment, as part of our safeguarding obligations towards pupils
- Support effective performance management
- Inform our recruitment and retention policies
- Allow better financial modelling and planning

7.3 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so. Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the School's Data Protection – Good Practice Guidelines.

8 SHARING PERSONAL DATA

During the course of our daily activities the School will frequently engage with third party organisations and may need to share personal data with them. A list of the third parties, with whom the School regularly shares data is available within Annex 1. The individuals concerned will be informed when the School shares personal data with third parties not on this list. The School will seek to ensure any third party upholds the principles of Data Protection as laid out in this document.

Personal data may be shared with a third party where:

- There is an issue with a pupil or parent/guardian that puts the safety of a pupil or our staff at risk
- We need to liaise with other agencies
    - to enable the relevant authorities to monitor the School's performance i.e. Independent Schools Inspectorate;
    - to compile statistical information (normally used on an anonymous basis);
    - to safeguard pupils' welfare and provide appropriate pastoral (and where relevant, medical and dental) care for pupils
    - where specifically requested by pupils and/or their parents or guardians;
    - to enable pupils to take part in national and other assessments and to monitor pupils' progress and educational needs;
    - where necessary in connection with learning and extra-curricular activities undertaken by pupils e.g. educational visits, peripatetic teachers, residential trip providers, extra-curricular providers;
    - to obtain appropriate professional advice
    - where a reference or other information about a pupil or ex-pupil is requested by another educational establishment or employer to whom they have applied;

- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT support, catering.
- The use by the School of online academic and educational services
- The use by the School of cloud IT services such as email and file storage for staff and pupils

- We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

    - The prevention or detection of crime and/or fraud
    - The apprehension or prosecution of offenders
    - The assessment or collection of tax owed to HMRC
    - In connection with legal proceedings
    - Where the disclosure is required to satisfy our safeguarding obligations

- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

We will only transfer personal data to a country or territory outside the European Economic Area if we are satisfied the third party(s) involved will only process the data in accordance with data protection law.

9 SUBJECT ACCESS REQUESTS AND OTHER RIGHTS OF INDIVIDUALS

9.1 Subject Access Requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the School holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject Access Requests must be submitted in writing, either by letter, email or fax to the Bursar.

They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

If staff receive a Subject Access Request they must immediately forward it to the Bursar.

9.2 Children and Subject Access

Requests

Personal data about a child belongs to that child, and not the child's parents or guardians. For a parent or guardian to make a Subject Access Request with respect to their child, the child must either be unable to understand their rights and the implications of a Subject Access Request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a Subject Access Request. Therefore, most Subject Access Requests from parents or guardians of pupils at the School may be granted without the express permission of the pupil. Children aged 12 and above may be mature enough to understand their rights and the implications of a Subject Access Request and therefore, a Subject Access Request from parents or guardians may require additional permission from the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- Will take appropriate steps to confirm the identity of the person making the request
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary and that they may seek redress with the Information Commissioner's Office if they feel this extension is not warranted

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

9.4 Other Data Protection Rights of the Individual

In addition to the right to make a Subject Access Request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- To request rectification of any data that is inaccurate or incomplete
- To have their personal data erased and to prevent further processing if:
    - It is no longer required for the purposes for which it was collected
    - Consent is withdrawn
    - There is an opposition to the processing and no superseding legitimate interest
- The personal data is being unlawfully processed
- The personal data must be removed in order to comply with a legal obligation
- Request a restriction of further processing of personal data
- Object to processing on specific grounds

Individuals should submit any request to exercise these rights to the Bursar. If staff receive such a request, they must immediately forward it to the Bursar.

10 PHOTOGRAPHS AND VIDEOS

As part of the School activities, we may take photographs and record images of individuals within the School. We will obtain written consent from parents/guardians for photographs and videos to be taken of their child and from staff for communication, marketing and promotional materials on an annual basis.

Uses may include:

- Within School on notice boards and in School magazines, brochures, newsletters, etc.
- Outside of School by external agencies such as the School photographer, prospectus, newspapers, campaigns
- Online on the School website, intranet or social media pages including Facebook, Twitter, Instagram, Flikr.

Consent will be sought for each specific use and can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video from all locations and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified, unless specific consent is provided.

See our Policy on Taking, Storing and Using Images of Children for more information on our use of photographs and videos.

11. DATA PROTECTION BY DESIGN AND DEFAULT

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)

- Completing Data Protection Impact Assessments where the School's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies

- Integrating data protection guidance and policy into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep records of attendance

- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant

- Maintaining records of our processing activities, including:

    - For the benefit of data subjects, making available the name and contact details of the School and all information we are required to share about how we use and process their personal data (via our privacy notices)

    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

12. DATA SECURITY AND STORAGE OF RECORDS

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records that contain personal data are kept under lock and key when not in use

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- iPads also have PIN codes. Staff are required to change their passwords at regular intervals.

- Personal information may only be stored on School devices, but staff and governors may access cloud-based services from their personal devices and are expected to follow the same security procedures as for School- owned equipment (see our IT Policy).

- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section

8)

13. DISPOSAL OF RECORDS

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the School's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

14. PERSONAL DATA BREACHES

The School will make all reasonable endeavours to minimise the risk of personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in Annex 2. When appropriate, we will report the data breach to the ICO within 72 hours.

15. TRAINING

All staff and management are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the School's processes make it necessary.

16. MONITORING ARRANGEMENTS

This policy will be reviewed and updated if necessary when the Data Protection Bill receives royal assent and becomes law – if any changes are made to the bill that affect the School's practice. Otherwise, or from then on, this policy will be reviewed **every 2 years.**

17. LINKS WITH OTHER POLICIES

This data protection policy is linked to our:

- Admissions Policy
- Anti-Bullying & Pastoral Care Policy
- Child Protection Policy including Policy on Taking, Storing and Using Images of Children
- Data Protection – Good Practice Guide including Retention of Records
- Equal Opportunities Policy
- First Aid Policy
- H&S Policy
- Induction Policy
- IT Policy
- Recruitment
- Registers Policy Admissions Policy
- SEN Policy

Annex 1: Third Party Data Processors

Following is a list of third party companies and organisations with whom the School regularly shares personal data:

Tapestry (on-Line assessment EYFS)

ISAMS (Management Information System)

Annex 2: Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the Bursar.

- The Bursar will investigate the report and determine whether a breach has occurred. To decide, the Bursar will consider whether personal data has been accidentally or unlawfully:
    - Lost
    - Stolen
    - Destroyed
    - Altered
    - Disclosed or made available where it should not have been
    - Made available to unauthorised people
- The Bursar will alert the Headmaster and the Proprietor

- The Bursar will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)

- The Bursar will assess the potential consequences, based on how serious they are, and how likely they are to happen

- The Bursar will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the Bursar will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:

    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

If it is likely that there will be a risk to people's rights and freedoms, the Bursar must notify the ICO.

- The Bursar will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Data Controller Log held on SharePoint
- Where the ICO must be notified, the Bursar will do this via the 'report a breach' page of the ICO website within 72 hours. As required, TITLE will set out:
    - A description of the nature of the personal data breach including, where possible:
        - The categories and approximate number of individuals concerned
        - The categories and approximate number of personal data records concerned
    - The name and contact details of the Bursar
    - A description of the likely consequences of the personal data breach

- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

- If all the above details are not yet known, the Bursar will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the Bursar expects to have further information. The Bursar will submit the remaining information as soon as possible
- The Bursar will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the Bursar will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the Bursar
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The Bursar will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The Bursar will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
  - Records of all breaches will be stored on the Data Controller Log held on SharePoint.
  - The Bursar and Headmaster will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to Minimise the Impact of Data Breaches

We will take the all necessary and practicable actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.