DANESMEAD, FULFORD CROSS, YORK YO10 4PB
TEL: (01904) 654983

YORK STEINER SCHOOL

DATA PROTECTION POLICY

Approved by:	Board of Trustees	**Date:**	July 2021
Last reviewed on:	**July 2021**		
Next review due by:	July 2023		

1. Aims

York Steiner School ('School') is committed to the protection of all personal data and special category personal data that we process as part of our school's activities, and to respect the privacy and rights of the individuals that we come into contact with.

Our School aims to ensure that all personal data collected about staff, pupils, parents, trustees, visitors and other individuals is collected, stored and processed in accordance with the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and Guidance

This policy meets the requirements of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) and the ICO's code of practice for subject access requests.

In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents/carers the right of access to their child's educational record.

3. Roles and Responsibilities

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

This policy does not form part of any school contract of employment and may be amended at any time.

3.1 Board of Trustees

The Board of Trustees has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

3.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.

The DPO will provide an annual report of their activities directly to the board of trustees and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose personal data the school processes and for the ICO.

Full details of the DPO's responsibilities are set out in their job description. Our DPO can be contacted via the School office.

3.3 School Business Manager

The School Business Manager (SBM) acts as the representative of the data controller and the DPO on a day-to-day basis.

3.4 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 a change of address;
- Contacting the DPO 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 need to rely on or capture consent, draft or update a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the United Kingdom (e.g. when planning an overseas trip);

- If there has been a personal data breach;
- If there has been an individual rights request;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;
- If they need help with any contracts or sharing personal data with third parties.

4. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: • Name (including initials), address & other contact details; • Identification number; • Location data; • Online identifier, such as a username. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: • Racial or ethnic origin; • Political opinions; • Religious or philosophical beliefs; • Trade union membership; • Genetics; • Health – physical or mental; • Sex life or sexual orientation.
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.

Data subject	The identified or identifiable individual whose personal data is held or processed (e.g. a member of staff).
Data controller	A person or organisation that determines the purposes and the means of processing of personal data (e.g. the school).
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 (e.g. a third-party supplier of the school).
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

5. The Data Controller

Our School processes personal data relating to parents, pupils, staff, trustees, visitors, suppliers and others and therefore is a data controller.

The School is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required. The School Business Manager (SBM) is the point of contact for the ICO.

6. Data Protection Principles

The DPA 2018 is based on data protection principles that our school must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner (transparency limitation);
- Collected for specified, explicit and legitimate purposes (purpose limitation);
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed (data minimisation);
- Accurate and, where necessary, kept up to date (data accuracy);
- Kept for no longer than is necessary for the purposes for which it is processed (storage limitation);
- Processed in a way that ensures it is appropriately secure (integrity and confidentiality - security).

In addition, the accountability principle requires us all to take responsibility for what we do with personal data and how we comply with the other principles. We must all ensure we have appropriate measures and records in place to be able to demonstrate our compliance.

This policy sets out how the school aims to comply with these principles.

7. Collecting Personal Data

7.1 Lawfulness, Fairness and Transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under the DPA 2018:

- The personal data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract (e.g. employment or purchasing contracts);
- The personal data needs to be processed so that the school can **comply with a legal obligation** (e.g. providing information to the Department of Education or Ofsted);
- The personal data needs to be processed to ensure the **vital interests** of the individual (e.g. to protect someone's life);
- The personal data needs to be processed so that the school, as a public authority, can perform a task **in the public interest,** and carry out its official functions (e.g. for teaching and research purposes);
- The personal 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) (e.g. alumni relations or fundraising);
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent** (e.g. the taking of, storage and use of images of pupils, i.e. photographs or videos).

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the DPA 2018.

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

In Relation to Consent:

Where none of the other bases for processing set out above apply then the School must seek the consent of the data subject before processing any personal data for any purpose. There are strict legal requirements in relation to the form of consent that must be obtained from data subjects.

When pupils and/or our workforce join the school a consent form will be required to be completed in relation to them. This consent form deals with the taking and use of photographs and videos of them, amongst other things. Where appropriate, third parties may also be required to complete a consent form.

In relation to all pupils under the age of 12 years old, we will seek consent from an individual with parental responsibility for that pupil. We will generally seek consent directly from a pupil who has reached the age of 12 however, we recognise that this may not be appropriate in certain circumstances and therefore may be required to seek consent from and individual with parental responsibility.

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

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

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

The DPO must always be consulted in relation to any consent form before consent is obtained. A record must always be kept of any consent, including how it was obtained and when.

7.2 Limitation, Minimisation and Accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their personal data.

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 and seek consent where necessary.

Staff must only process personal data where it is necessary in order to fulfil their role within the school and not use it for any other purpose.

When staff no longer need the personal data they hold, they must ensure it is deleted, confidentially destroyed (if a paper record) or anonymised, and care must be taken in relation to where it is retained. This will be done in accordance with the School's records retention policy.

8. Sharing Personal Data

We will not normally share personal data with anyone else, but may do so where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- We need to liaise with outside agencies which support schools – we will seek consent as necessary before doing this;
- Our suppliers or contractors need personal data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
    - Establish a personal data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share;
    - Only share personal data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

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, staff or other individuals.

Where we transfer personal data to a country or territory outside the United Kingdom, we will do so 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 personal data (but not to a record or a document);
- The purposes of the personal data processing (e.g. employment purposes or education provision purposes);
- The categories of personal data concerned;
- Who the personal data has been, or will be, shared with;
- How long the personal data will be stored for, or if this isn't possible, the criteria used to determine this period;
- The source of the personal data, if not the individual;
- Whether any automated decision-making is being applied to their personal data, and what the significance and consequences of this might be for the individual (note, the school does not carry out any automated decisions).

We would prefer that subject access requests are submitted in writing (as against verbally), either by letter or email to the School Business Manager (SBM). They should include:

- Name of individual;
- Correspondence address;

- Contact number and email address;
- Details of the information requested in as much detail as possible to aid searches.

If staff receive a subject access request, they must immediately forward it to the SBM, as the school only has a calendar month from date of receipt to respond, unless specific circumstances are present.

9.2 Children and Subject Access Requests

Personal data about a child belongs to that child and not the child's parents or carers. For a parent or carer 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 carers of pupils at our school may be granted without the express permission of 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.

Children aged 12 and above are generally 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 carers of pupils at our school will not be granted without the express permission of 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. For that reason, an assessment with the DPO (and as appropriate, the Designated Safeguarding Lead or a member of the Safeguarding team) will be conducted before the pupil is approached for consent.

If a subject access request is received directly from a pupil, it will be treated like any other subject access request except that the DPO will be entitled to liaise with a member of the Safeguarding team.

9.3 Responding to Subject Access Requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made;
- 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;
- 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 personal data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time;
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Challenge processing which has been justified on the basis of public interest;
- Request a copy of agreements under which their personal data is transferred outside of the United Kingdom;
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them);
- Prevent processing that is likely to cause damage or distress;

- Be notified of a data breach in certain circumstances;
- Make a complaint to the ICO;
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the School Business Manager (SBM). If staff receive such a request, they must immediately forward it to the SBM.

10. Parental Requests to See the Educational Record.

Parents/carers, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 1 month of receipt of a written request.

11. Photographs and Videos

As part of our school activities, we may take photographs and record images of individuals within our school. We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

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, newspapers, campaigns;
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video 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.

12. Data Protection by Design and Default

We will put measures in place to show that we have integrated, as appropriate, data protection principles into all relevant data processing activities, including:

- Appointing a suitably qualified DPO and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- 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 privacy 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 (the DPO will advise on this process);
- Integrating data protection 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 a record of attendance;
- Regularly conducting reviews and assessments 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 our school and those responsible for data protection matters on a day to day basis, 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 personal data, data subject, how and why we are using the personal data, any third-party recipients, how and why we are storing the personal data, retention periods and how we are keeping the personal data secure.

13. 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 and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use;
- Papers containing confidential or 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;

- Where personal data needs to be taken off site, staff are responsible for ensuring its confidentiality and security whilst off site and its safe return to site;
- Documents containing personal data must be collected immediately from printers and not left on photocopiers;
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff are reminded to change their passwords at regular intervals;
- Users of monitors must ensure that individual monitors do not show personal data to passers-by and that they log off from their laptop or other device when it is left unattended;
- Staff, pupils or trustees who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (note however, if a subject access request is received, individual's personal devices may need to be searched to satisfy the request);
- 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).

14. 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 or incinerate 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.

15. Personal Data Breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected personal data breach, we will follow the procedure set out in Appendix 1.

When appropriate, we will report the personal data breach to the ICO within 72 hours and/or take steps to inform any impacted individuals. Such breaches in a school context may include, but are not limited to:

- Safeguarding information being made available to an unauthorised person;
- The theft of a school laptop containing non-encrypted personal data about pupils.

16. Training

All staff and trustees 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.

17. Monitoring Arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed **annually** and if there are any material changes, will be shared with the Board of Trustees for approval.

Appendix 1: Personal Data Breach Procedure

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

- On finding or causing a personal data breach, or potential personal data breach ('a breach'), the staff member or data processor must immediately notify the DPO;

- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO 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 DPO will alert the School Business Manager and/or the Education Manager and the Chair of Trustees;

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

- The DPO 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 DPO will consider whether the breach is likely to negatively affect individual'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 personal data;
  - Discrimination;
  - Identify theft or fraud;
  - Financial loss;
  - Unauthorised reversal of pseudonymisation (for example, key-coding);
  - Damage to reputation;

- Loss of confidentiality;
- Any other significant economic or social disadvantage to the individual(s) concerned.

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

- The DPO 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;

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the 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 DPO;
  - A description of the likely consequences of the 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 DPO 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 DPO expects to have further information. The DPO will submit the remaining information as soon as possible;

- The DPO 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 DPO 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 DPO;
  - A description of the likely consequences of the 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.

- The DPO 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 DPO 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 in paper form by the School Business Manager (SBM) and also on the school's Dropbox account.

The DPO and relevant School Managers 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 Personal Data Breaches

We will take the actions set out below to mitigate the impact of different types of 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 breach.

Sensitive Information Being Disclosed via Email (including Safeguarding Records)

- If special category personal data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error;

- Members of staff who receive sensitive information sent in error must alert the sender and the DPO as soon as they become aware of the error – it should either be returned to the sender (securely) or deleted and not used for any purpose;

- In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error and request that those individuals confidentially destroy or delete the information and do not share, publish, save or replicate it in any way;

- The DPO will ensure we receive a written response from all the individuals who received the sensitive information, confirming that they have complied with this request;

- The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.