Data Protection Policy

Policy Number:	YH013
Version:	V1
Date of issue:	September 2021
Date of Review:	September 2022
Responsible Person:	Head of Finance and Support Services
Ratified by:	Alfred Foglio – Chair of the Board of Directors
Outcome:	The purpose of the plan is to: • Ensure that all personal data collected about staff, students, parents, directors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation and the EU General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018").

EQUALITY AND DIVERSITY STATEMENT

Under the Equality Act 2010 we have a duty not to discriminate against people on the basis of their age, disability, gender, gender identity, pregnancy or maternity, race, religion or belief and sexual orientation. This policy has been equality impact assessed and we believe that it is in line with the Equality Act 2010 as it is fair, it does not prioritise or disadvantage any employee or applicant and it helps to promote equality at this school

Table of Contents

1. Aims

Yarrow Heights School ("our School") aims to ensure that all personal data collected about staff, students, parents, trustees, directors , visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation and the EU General Data Protection Regulation ("GDPR") and 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 GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR.

This policy meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data.

This policy also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with our Funding Agreement and Articles of Association.

3. Definitions

term	definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: ✓ Name (including initials) ✓ 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 ✓ Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ✓ 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.
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.

4. Data Controller

Our School determines the purposes and means of processing personal data relating to parents, students, staff, trustees, directors, visitors and others, and is therefore the data controller.

Our School is registered as data controller in the UK with the Information Commissioner's Office, registration number ZA915011.

5. Roles and responsibilities

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

6. Board of Directors

The Board of Directors for our School has overall responsibility for ensuring that the School complies with all relevant data protection obligations.

7. 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. The DPO is the contact point for the ICO.

They will provide an annual report of their activities directly to the Board of Directors and, where relevant, report to the board their advice and recommendations on School data protection issues.

The School has appointed a Data Protection Manager (DPM) who acts as a first point of contact for individuals whose data the School processes and who deals with general day-to-day data protection enquiries. The DPM will contact the DPO for advice and guidance when necessary.

Our DPO is contactable via email at reception@yarrowheights.com .

a. Headteacher

The Headteacher at Yarrow Heights School acts as the Senior Information Risk Owner (SIRO) for the School and is representative for the data controller on a day-to-day basis.

b. 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 DPM 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 they have a lawful basis to use personal data in a particular way.
    - ➢ If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.
    - ➢ If there has been a data incident, data breach or near miss.

- 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.

8. **Data protection principles**

The GDPR is based on data protection principles. The principles say that personal data must be:

- ✓ Processed lawfully, fairly and in a transparent manner.
- ✓ Collected for specified, explicit and legitimate purposes.
- ✓ Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.
- ✓ Accurate and, where necessary, kept up to date.
- ✓ Kept for no longer than is necessary for the purposes for which it is processed.
- ✓ Processed in a way that ensures it is appropriately secure.

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

9. **Collecting personal data**

a. Lawfulness, fairness and transparency

Our School will only process personal data where they have one of six '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 the individual has asked the School to take specific steps before entering 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 or another person i.e. to protect someone's life.
- ✓ The data needs to be processed so that the School, as a public authority, can **perform a task in the public interest or exercise its official authority.**
- ✓ The data needs to be processed for the **legitimate interests** of the School (where the processing is not for any tasks the School performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
- ✓ The individual (or their parent/carer when appropriate in the case of a student) has freely given clear **consent.**

For special categories of personal data, the School will also meet one of the special category conditions for processing under data protection law:

- ✓ The individual (or their parent/carer when appropriate in the case of a student) has given **explicit consent.**

- ✓ The data needs to be processed to perform or exercise obligations or rights in relation to **employment, social security or social protection law.**
- ✓ The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- ✓ The data has already been made **manifestly public** by the individual.
    - ✓ The data needs to be processed for the establishment, exercise or defence of **legal claims.**
    - ✓ The data needs to be processed for reasons of **substantial public interest** as defined in legislation.
    - ✓ The data needs to be processed for **health or social care purposes**, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law.
    - ✓ The data needs to be processed for **public health reasons**, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law.
    - ✓ The data needs to be processed for **archiving purposes**, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest.

For criminal offence data, the School will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- ✓ The individual (or their parent/carer when appropriate in the case of a student) has given **consent.**
- ✓ The data needs to be processed to ensure the **vital interests** of the individual or another person, where the individual is physically or legally incapable of giving consent.
- ✓ The data has already been made **manifestly public** by the individual.
- ✓ The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of **legal rights.**
- ✓ The data needs to be processed for reasons of **substantial public interest** as defined in legislation.

Whenever our School first collects personal data directly from individuals, they will provide them with the relevant information required by data protection law.

Our School will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

b. Limitation, minimisation and accuracy

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

If the School wishes to use personal data for reasons other than those given when first obtaining 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 do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be carried out in accordance with the School's Personal Data Retention and Destruction Policy and Schedule.

10. Sharing personal data

Our School will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

✓ There is an issue with a student or parent/carer that puts the safety of staff at risk.

✓ We need to liaise with other agencies - we will seek consent as necessary before doing this.

✓ Suppliers or contractors need data to enable our School to provide services to staff and students – 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 contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share.

✓ Only share data that the supplier or contractor needs to carry out their service.

We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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 students or staff.

Where our School transfer personal data internationally, they will do so in accordance with data protection law.

11. Subject access requests and other rights of individuals

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.
- ✓ With whom the data has been, or will be, shared.

- ✓ How long the data will be stored, or if this is not possible, the criteria used to determine this period.
- ✓ Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing.
- ✓ The right to lodge a complaint with the ICO or another supervisory authority.
- ✓ The third-party 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.
- ✓ The safeguards provided for international data transfers, if applicable.

Subject access requests can be submitted in any form, but we may be able to respond to requests quicker if they are made in writing and include:

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

If staff receive a subject access request in any form, they must immediately forward it to the DPM for assessment and potential escalation to the DPO.

Children and subject access requests

Personal data about a child belongs to that child, and not to 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 aged 12 and under are generally not regarded as being mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of students of this age within our School may be granted without the express permission of the student.

Children aged 13 and over 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 students of this age within our School may not be granted without the express permission of the student.

In both cases noted above, this is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

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 (or receipt of any additional information needed to confirm identity, where relevant).
- ✓ 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 may not disclose information for a variety of reasons, such as if it:

- ✓ Might cause serious harm to the physical or mental health of the student 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
- ✓ Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- ✓ Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

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:

- ✓ 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
- ✓ Object to processing which has been justified on the basis of public interest, official authority or legitimate interests
- ✓ Challenge processing which has been justified on the basis of public interest
- ✓ Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)

- ✓ 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 DPM. If staff receive such a request, they must also immediately forward it to the DPM.

Parental requests to see the educational record

Parents, or those with parental responsibility, can request free access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request. If the request is for a copy of the educational record, charges may be applicable (as set out in the Freedom of Information Policy).

This applies if the student concerned is aged under 18.

There are certain circumstances in which this access can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the student or another individual, or if it would mean releasing exam marks before they are officially announced.

Photographs and videos

As part of our School activities, we may take photographs and record images of individuals within our School.

Students aged 12 and under

Our School will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. They will clearly explain how the photograph and/or video will be used to both the parent/carer and student.

Any photographs and videos taken by parents/carers at School events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this in writing. This consent will be renewed annually, and parents/carers will be asked to advise the School should the situation change.

Students aged 13 and over

Our School will obtain written consent from parents/carers, and students themselves for photographs and videos to be taken of students for communication, marketing and promotional materials. This consent will be renewed annually, and all parties will be asked to advise the School should the situation change.

Where they need parental consent, the School will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where they don't need parental consent, our School will clearly explain to the student how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at School events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other students are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or students where appropriate) have agreed to this.

Refusal / Withdrawal of consent

Consent can be refused or withdrawn at any time. If consent is withdrawn, our School will delete the photograph(s) or video(s) and not distribute it/them further.

Data protection by design and default

Our School will put measures in place to show that we have integrated data protection into all our 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 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 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 audits to test privacy measures and make sure they are compliant.
- ✓ Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will apply
- ✓ Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our School's DPO and all information they are required to share about how they use and process their personal data (via privacy notices)
    - For all personal data that our School holds, maintaining an internal record of the type of data, type of data subject, how and why they are using the data, any third-party recipients, any transfers outside of the EEA and the safeguards for those, retention periods and how they are keeping the data secure.

Data security and storage of records

Our School 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. The following policies are available upon request which outline the security procedures in place throughout our School:

- ✓ Data Handling Security Policy
- ✓ IT Credentials Management Policy
- ✓ Portable Device Policy
- ✓ Records Management Policy

Disposal of records

Personal data that is no longer needed will be disposed of securely in accordance with our Personal Data Retention and Destruction Policy and Schedule. Personal data that has become inaccurate or out of date will also be disposed of securely, where the School cannot or do not need to rectify or update it.

For example, the School will shred or incinerate paper-based records and overwrite or delete electronic files. They may also use a third party to safely dispose of records on the School's behalf. If the School do so, they will require the third party to undertake assurances that it complies with data protection law.

Personal data breaches

In the unlikely event of a data incident, a data breach, or a near miss, we will follow the procedure set out in our Personal Data Breach Procedure.

When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Such breaches in a School context may include, but are not limited to:

- A non-anonymised dataset being published on the School website which shows the exam results of students eligible for the student premium.
- Safeguarding information being made available to an unauthorised person.
- The theft of a School laptop containing non-encrypted personal data about students.

All staff and directors 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.

Monitoring arrangements

This policy will be reviewed annually by the Board of Directors and the DPO.

This policy will be reviewed annually by the Board of Directors and the DPO and updated if necessary, for example if any further changes are made to data protection legislation that affect our School's practice.

Links with other policies

This data protection policy is linked to our:

- ✓ Data Protection by Design and DPIA Policy
- ✓ Personal Data Retention and Destruction Policy and Schedule
- ✓ Data Subject Rights Request Procedure
- ✓ Personal Data Breach Procedure
- ✓ DPIA Procedure
- ✓ Employee Data Protection Code of Conduct
- ✓ Freedom of information publication scheme
- ✓ Surveillance Management Procedure
- ✓ E-Safety Policy
- ✓ Acceptable Use Policy
- ✓ Data Handling Security Policy
- ✓ IT Credentials Management Policy
- ✓ Portable Storage Device Policy
- ✓ Security Incidents Policy
- ✓ Biometrics Policy
- ✓ Statutory Requests for Information Policy
- ✓ Freedom of Information

APPENDIX 1 : School contact details

For any School specific queries regarding data protection. For any School related queries please email reception@yarrowheights.com .