JESSIE YOUNGHUSBAND SCHOOL

Data Protection Policy

Updated summer 2020
Review summer 2022

Aspire ~ Respect ~ Enjoy

1. Introduction

1.1 Jessie Younghusband School collects and uses certain types of personal information about staff, students, parents, governors, visitors and other individuals who come into contact with the school in order to provide education and associated functions.

1.2 Jessie Younghusband School aims to ensure that all personal data is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the UK Data Protection Act 2018.

2. Document purpose

2.1 The purpose of the policy is to:

- Set out the manner in which personal data of staff, students, parents, governors and other individuals is processed fairly and lawfully, and in compliance with the data protection principles;
- Inform all staff involved in the collection, processing and disclosure of personal data of their duties and responsibilities under this policy;
- Instil confidence in the school's ability to process personal data fairly and securely.

3. Scope

3.1 This policy applies to the personal data of all Jessie Younghusband School employees, governors, students, parents and carers, volunteers and any other person carrying out activities on behalf of the school.

3.2 It applies to the processing of all personal data, whether it be in paper form or electronic computerised data.

4. Key definitions

4.1 Key data protection definitions are detailed in the table below:

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's name (including initials), identification number, location data and 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.
GDPR Special Category 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 'living' 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 e.g. the 'why' and the 'how'.
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.

5. Data Controller

5.1 The School is a data controller and must therefore comply with the data protection principles detailed below in the processing of personal data, including the way in which the data is obtained, stored, used, disclosed and destroyed.

5.2 The School's Information Commissioner's Office (ICO) registration number is Z6058022.

6. Data Protection Principles

6.1 The GDPR is based on data protection principles that the school must comply with. The principles state 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.

6.2 In addition to this, Jessie Younghusband School will have in place a process for dealing with the exercise of the following rights by Governors, staff, parents and carers, and members of the public in respect of their personal data:

- to be informed about what data is held, why it is being processed and who it is shared with;
- to access their data;
- to rectification of the record;
- to erasure;
- to restrict processing;
- to data portability;
- to object to processing;
- not to be subject to automated decision-making including profiling.

7. Roles and Responsibilities

7.1 The Governing Body of the School and the Head Teacher are responsible for implementing good data protection practices and procedures within the School and for compliance with the data protection principles.

7.2 The School's **Data Protection Officer (DPO)** has responsibility for all issues relating to the processing of personal data and will report directly to the Head Teacher. The DPO's contact details can be found at Section 18.

7.3 The DPO will comply with responsibilities under the GDPR and deal with subject access requests, requests for rectification and erasure, and data security breaches. Complaints about data processing will be dealt with in accordance with the School's Complaints Policy.

7.4 It is the responsibility of **all staff** to ensure that their working practices comply with the data protection principles. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures forming part of this policy.

7.5 Failure to comply with the data protection principles exposes the School and staff to civil and criminal claims and possible financial penalties.

8. Compliance with the principles

8.1 Jessie Younghusband School is committed to complying with the data protection principles outlined above. This means that the School will:

- inform individuals as to the purpose of collecting any information from them, as and when we ask for it, including publishing Privacy Notices where appropriate;
- be responsible for checking the quality and accuracy of the information it holds;
- regularly review the records held to ensure that information is not held longer than is necessary, and that it has been held in accordance with the 'Information and Records Management Society Tool Kit for Schools'.
- ensure that when information is authorised for disposal it is done appropriately;
- ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system;
- share personal information with others only when it is necessary and legally appropriate to do so;
- set out clear procedures for responding to requests for access to personal information known as subject access requests; and
- report any suspected data breaches in accordance with the procedure in Section 17 below.
- Ensure staff understand our policies and procedures, by providing regular data protection awareness training, including at new staff inductions.

9. Conditions for processing

9.1 The School will only process personal data where it has one of six lawful bases (legal reasons) to do so under data protection law:

- **Public task** - so that it can perform a task in the public interest and carry out its official functions e.g. deliver education and learning;
- **Legal obligation** - so that it can comply with a legal obligation;
- **Fulfilling a contract** - so that the school can fulfil a contract with an individual;

- **Vital interest** - to ensure the vital interests of an individual e.g. to protect someone's life;
- **Legitimate interest** - share data outside the scope of delivering education and learning, but within the realms of what a data subject would reasonably expect, provided the individual's rights and freedoms are not overridden;
- **Consent** - where an individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

10. Sharing personal data

10.1 Jessie Younghusband School will share personal data with appropriate authorities and third parties such as law enforcement and government bodies e.g. Department for Education, where it is fair and lawful to do so.

10.2 The School may also share personal data with various third-party suppliers and contractors. In such cases we will:

- only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law;
- establish a data sharing agreement with the supplier or contractor, either in the commercial contract or as a standalone agreement, 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.

10.3 The School 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.

10.4 If we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

11. Subject Access Request

11.1 Individuals have a right to make a Subject Access Request (SAR) to gain access to personal information that the School holds about them.

11.2 Subject Access Requests should ideally be submitted in writing, either by letter or email, to the School's Data Protection Officer. Written requests should include:

- name of individual making the request;
- date and time that the request was made;
- correspondence address;
- contact number and email address;
- details of the information requested - with specific time periods where applicable.

11.3 When responding to requests, the School:

- may ask the individual to provide two forms of identification;
- may contact the individual via phone to confirm the request was made;
- will respond without delay and within **one month** of receipt of the request (once proof of identification has been received where appropriate);
- will provide the information free of charge;
- may tell the individual that the School will comply within three months of receipt of the request, where a request is complex or numerous. The School will inform

the individual of this within one month and explain why the extension is necessary.

11.4 The School 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.

12. Other rights of individuals

12.1 Under data protection law, individuals also have other rights regarding how their personal data is used and kept safe, including the right to:

- object to the use of personal data if it would cause, or is causing, damage or distress;
- prevent it being used to send direct marketing;
- object to decisions being taken by automated means (by a computer or machine, rather than by a person);
- ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances);
- be notified of a data breach in certain circumstances;
- a right to seek readdress, either through the Information Commissioner's Office (ICO), or through the courts.

12.2 Individuals, whether they be staff or parents/carers, should submit any request to exercise these rights to the Data Protection Officer in the first instance. It such requests are made to other staff they should be forward to the DPO at the earliest possible time.

13. Photographs, videos and media

13.1 As part of school activities, Jessie Younghusband may take photographs or videos and on occasion allow external organisations to take photographs or to film within the school. In the case of external organisations, whether it be a local photography firm or the media, Pp/carers will be made aware when this is happening and the context in which the photograph or will be used. Consent will be sought if a child's photograph/images are to be take/recorded.

13.2 The school will take photographs or videos for its own use. Usually these will be unnamed and will generally be for internal school use, but on occasion such images may be published and accessible by the wider public, such as:

- Photographs included in a school prospectus;
- Photographs to show as slides at an event for parents/carers;
- Photographs to be used on display boards, which can be seen by visitors to the school;
- Photographs posted on the school's official websites such as Twitter and Facebook sites.

13.3 It is important to note that any photographs or video images that can be accessed by the public will be monitored closely by school staff to ensure they are appropriate.

13.4 Named photographs will be used for internal use where there is a clear lawful basis for doing so e.g. safeguarding requirements or part of exclusion behaviour data. For all other purposes, if the school wants to use named photographs then it will obtain specific parent/carer consent first.

14. Data protection by design and default

14.1 The School 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;
- completing Data Protection Impact Assessments (DPIA) 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. All new staff and governors will be provided with data protection training as part of their induction process;
- All staff are to read and sign to state they have understood the School's Acceptable Use of ICT Policy.

15. Data security and storage of records

15.1 The 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. In particular:

- paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data (where authorised) are kept under lock and key when not in use;
- access to personal data will only be given to those who need access for the purpose of their duties;
- 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. Where there is a health and safety requirement to display such information e.g. Medical Health Care Plans, then every consideration must be given to reduce the risk of the document being seen by those not authorised;
- passwords that are at least eight characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students (where applicable) are reminded to change their passwords at regular intervals;
- encryption software is used to protect all portable devices and removable media, such as laptops and USB devices (where authorised);
- staff, students or Governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment;

- where we need to share personal data with a third party, we will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected.

16. Disposal of records

16.1 Personal data that is no longer needed will be disposed of securely in accordance with timelines specified in the 'Information and Records Management Society Retention Guidelines for Schools'. 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.

16.2 The School may use a third party to safely dispose of records. If this is the case, then we will require the third party to provide sufficient guarantees that it complies with data protection law.

17. Personal data breaches

17.1 A personal data incident occurs when there is an event giving rise to the potential for accidental, unauthorised or unlawful access, acquisition, alteration, destruction, disclosure, loss or misuse of personal data. For example:

- pupil medical details disclosed by email to unauthorised individuals;
- attendance reports and student assessments sent to the wrong parents;
- staff data sent to unauthorised external email accounts;
- trip assessments, including medical and behaviour information, left on coaches or lost;
- confidential documents containing personal data stolen from a car boot;
- using 'Cc' to send emails to multiple parents so that personal email addresses are visible to everyone;
- confidential personal data being accessible to everyone on the School IT network;
- the loss of personal data shared with a third party following a cyber-attack.

17.2 The School will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the Data Protection Officer should be notified at the earliest possible time, so it can be dealt with in accordance with the School's 'Data Incident Management' process.

17.3 When appropriate i.e. if there is a high risk to the rights of the individual, data breaches will be reported to the ICO within **72 hours** of the School becoming aware of them.

17.4 It is important that all staff report a breach or suspected breach at the earliest possible time. Not reporting an incident or suspected personal data breach is as detrimental as not reporting it all, as the School will not be able to isolate and mitigate risks and learn the lessons.

18. Data Protection Officer's Contact details

18.1 The School Business Manager is the Data Protection Officer and she can be contacted at: **dpo@jys.org.uk**.

Annex A: Guidance to staff when handling personal data

What staff should do:

DO get the permission of your line manager before taking any confidential information home.

DO transport information from the School on secure computing devices (i.e. encrypted laptops and encrypted memory sticks if authorised). Wherever possible avoid taking paper documents out of the office.

DO use secure portable computing devices such as encrypted laptops when working remotely or from home.

DO ensure that all paper-based information that is taken off the School premises is kept confidential and secure, ideally in a sealed envelope which indicates a return address if misplaced.

DO ensure that any confidential documents that are taken to your home are stored in a locked drawer.

DO ensure that paper-based information and laptops are kept safe and close to hand when taken off school premises. Never leave them unattended.

DO ensure that when transporting paper documentation in your car that it is placed in the boot (locked) during transit.

DO return the paper-based information to the School as soon as possible and file or dispose of it securely.

DO report any loss of paper-based information or portable computer devices to your line manager and the Data Protection Officer immediately.

DO ensure that all postal and e-mail addresses are checked to ensure safe dispatch of information.

DO use pseudonyms and anonymise personal data where possible.

DO ensure that access to SIMS is restricted to appropriate staff only and that leavers are removed in a timely manner.

What staff must not do:

DO NOT take confidential information to an entertainment or public place such as a pub or cinema, whether held on paper or an electronic device.

DO NOT unnecessarily copy other parties into e-mail correspondence.

DO NOT e-mail documents to your own personal computer.

DO NOT store work related documents on your home computer, especially if they contain personal data.

DO NOT leave personal information unclaimed on any printer.

DO NOT leave personal information on your desk overnight, or if you are away from your desk for prolonged periods.

DO NOT leave documentation in vehicles overnight.

DO NOT discuss case level issues at social events or in public places.

DO NOT put confidential documents in non-confidential recycling bins.

DO NOT print off reports with personal data (e.g. pupil data) unless absolutely necessary.

DO NOT use unencrypted memory sticks or unencrypted laptops. Use of such devices must be authorised.