Data Protection Policy

April 2019

THE JO RICHARDSON

SUCCESS FOR ALL

COMMUNITY SCHOOL

ACHIEVE

Introduction

Jo Richardson Community School (JRCS) is fully committed to compliance with the requirements of the General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018 (DPA). The School will therefore, follow procedures which aim to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is processed fairly, lawfully and transparently.

The General Data Protection Regulation (GDPR) ensures a balance between an individual's rights to privacy and the lawful processing of personal data undertaken by organisations in the course of their business. It aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The School will protect and maintain a balance between data protection rights in accordance with the GDPR. This policy sets out how we handle the personal data of our staff, pupils, parents, governors, visitors and other individuals.

The school will therefore, follow procedures that aim to ensure that all individuals permitted to access personal data held by or on behalf of JRCS is fully aware of, and abides by their duties and responsibilities under the GDPR and DPA. All individuals employed by JRCS will agree to undertake any relevant training that may be appropriate to the role being undertaken.

Scope

This policy applies to the collection and processing of all personal data held by the school, falling within the scope of the GDPR and the DPA, in all formats including paper, electronic, audio and visual. It applies to all staff, governors, volunteers and contractors.

Definitions

Data subject

The data subject is an individual about whom such information is collected and stored.

Data Controller

The Data Controller is the person who (either alone or jointly or in common with other persons) determines the purposes and manner for which personal data are or are to be processed. The Head of School is the Data Controller for JRCS.

Personal data

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special category data

Previously termed "sensitive personal Data", special category data is similar by definition and refers to data concerning an individual data subject's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Although there are clear distinctions between personal and special category data, for the purposes of this policy the term 'personal data' refers equally to 'special category data' unless otherwise stated.

The GDPR and DPA rules for special category data do not apply to information about criminal allegations, proceedings, or convictions. Instead, there are separate safeguards for personal data relating to criminal convictions and offences, or related security measures.

Processing
Processing data involves any activity that involves the use of personal data. This includes but is not limited to: obtaining, recording or holding data or carrying out any operation or set of operations on that data such as organisation, amending, retrieving using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Automated processing
Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

An example of automated processing includes profiling and automated decision-making. Automatic decision-making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision-making is prohibited except in exceptional circumstances.

Data Protection Impact Assessment (DPIA)
A DPIA is a tool used to identify risks in data processing activities with a view to reducing them.

Criminal records information
This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures.

Processing Personal Data

Data protection principles
The School is responsible for and adheres to the principles relating to the processing of personal data as set out in the GDPR.

The principles the School must adhere to are:

(1) Personal data must be processed lawfully, fairly and in a transparent manner;
(2) Personal data must be collected only for specified, explicit and legitimate purposes;
(3) Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
(4) Personal data must be accurate and, where necessary, kept up to date;
(5) Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed; and
(6) Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

Further details on each of the above principles is set out below.

Principle 1: Personal data must be processed lawfully, fairly and in a transparent manner
The School only collect, process and share personal data fairly and lawfully and for specified purposes. The School must have a specified purpose for processing personal data and special category data as set out in the GDPR.

Before the processing starts for the first time, we will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. We will then regularly review

those purposes whilst processing continues in order to satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie, that there is no other reasonable way to achieve that purpose).

Personal Data

The School may only process a data subject's personal data if one of the following fair processing conditions are met: -

- The data subject has given their consent;
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- To perform a task in the public interest or in order to carry out official functions as authorised by law;
- For the purposes of the School's legitimate interests where authorised in accordance with data protection legislation. This is provided that it would not prejudice the rights and freedoms or legitimate interests of the data subject.

Special Category Data

The School may only process special category data if they are entitled to process personal data (using one of the fair processing conditions above) AND one of the following conditions are met: -

- The data subject has given their explicit consent;
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the School in the field of employment law, social security law or social protection law. This may include, but is not limited to, dealing with sickness absence, dealing with disability and making adjustments for the same, arranging private health care insurance and providing contractual sick pay;
- To protect the data subject's vital interests;
- To meet our legal compliance obligations (other than a contractual obligation);
- Where the data has been made public by the data subject;
- To perform a task in the substantial public interest or in order to carry out official functions as authorised by law;
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services;
- Where it is necessary for reasons of public interest in the area of public health;
- The processing is necessary for archiving, statistical or research purposes.

The School identifies and documents the legal grounds being relied upon for each processing activity.

Consent

Where the School relies on consent as a fair condition for processing (as set out above), it will adhere to the requirements set out in the GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (ie, more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the School will normally seek another legal basis to process that data. However, if explicit consent is required, the data subject will be provided with full information in order to provide explicit consent.

The School will keep records of consents obtained in order to demonstrate compliance with consent requirements under the GDPR.

Principle 2: Personal data must be collected only for specified, explicit and legitimate purposes
Personal data will not be processed in any matter that is incompatible with the legitimate purposes.

The School will not use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the data subject of the new purpose (and they have consented where necessary).

Principle 3: Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
The School will only process personal data when our obligations and duties require us to.

We will not collect excessive data and ensure any personal data collected is adequate and relevant for the intended purposes.

When personal data is no longer needed for specified purposes, the School shall delete or anonymise the data.

Principle 4: Personal data must be accurate and, where necessary, kept up to date
The School will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out of date personal data.

Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the School.

Principle 5: Personal data must not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed
Legitimate purposes for which the data is being processed may include satisfying legal, accounting or reporting requirements. The School will ensure that they adhere to legal timeframes for retaining data.

We will take reasonable steps to destroy or erase from our systems all personal data that we no longer require. We will also ensure that data subjects are informed of the period for which data is stored and how that period is determined in our privacy notices.

Please refer to the School's Retention Policy for further details about how the School retains and removes data.

Principle 6: Personal data must be processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage
In order to assure the protection of all data being processed, the School will develop, implement and maintain reasonable safeguarding and security measures. This includes using measures such as: -

- Encryption;
- Pseudonymisation (this is where the School replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure);
- Ensuring authorised access (ie, that only people who have a need to know the personal data are authorised to access it);
- Adhering to confidentiality principles;
- Ensuring personal data is accurate and suitable for the purpose for which it is processed.

The School follows procedures and technologies to ensure security and will regularly evaluate and test the effectiveness of those safeguards to ensure security in processing personal data.

The School will only transfer personal data to third party service providers who agree to comply with the required policies and procedures and agree to put adequate measures in place.

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 other agencies – we will seek consent as necessary before doing this;
- Our suppliers or contractors need 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 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 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 or staff.

Transfer of data outside the European Economic Area (EEA)

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

The School will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the GDPR. All staff must comply with the School's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when you transmit, send, view or access that data in that particular country.

Data subject's rights

The school recognises that access to personal data held about an individual is a fundamental right provided in the Act. These rights include:

- The right to be informed;
- The right of access to personal information;
- The right to request rectification;
- The right to request erasure;
- The right to restrict processing in certain circumstances;
- The right to data portability;
- The right to object to processing;
- Rights to automated decision-making including profiling.

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. This is not a rule and a pupil's ability to understand their rights will always be judged on a case by-case basis.

The school will ensure that all requests from individuals to access their personal data are dealt with as quickly as possible and within the one calendar month in the legislation, as long as the data subject meets the requirements set out in this policy.

To minimise delays and unnecessary work all requests from data subjects must:

- Be made in writing (paper or email) to gdpr@jorichardson.org.uk;
- Be accompanied by adequate proof of the identity of the data subject where required and, where applicable, the written authorisation of the data subject (if the request is being made on their behalf by a legal or lawfully appointed representative or, authorised agent);
- Specify clearly and simply the information required;
- Give adequate information to enable the requested data to be located;
- Make it clear where the response should be sent.

The Data Protection Officer must be informed of any request to action against one or more of these rights.

The Act allows exemptions from providing information to individuals making a subject access request, and non-disclosure of information, in specific and limited circumstances. The school will normally apply the exemptions and the non-disclosure of information rules, unless it is satisfied that it is appropriate or reasonable not to do so and, in any event, will always do so in circumstances where it is deemed necessary to the effective operation of the school, for the prevention and detection of crime, to protect the individual or is required by law.

If a data subject remains dissatisfied with a response received, they may ask for the matter to be reviewed, or, in the case of an employee, through the school's grievance process. Ultimately if a data subject continues to be dissatisfied, she/he has the right to ask the Information Commissioner's Office (ICO) to carry out an assessment of their case and/or pursue a legal remedy.

CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Further information about the school's CCTV system can be found in our CCTV policy.

Biometric recognition systems

Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school meals instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

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 data breach, we will follow the procedure we have put in place and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the ICT Systems and Network Manager who is the person designated as the key point of contact for personal data breaches. In the absence of the ICT Network and Systems Manager, please contact the Head of School or Headteacher.

Privacy by design
The School adopts a "privacy by design" approach to data protection to ensure that we adhere to data compliance and to implement technical and organisational measures in an effective manner.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. To help us achieve this, the School takes into account the nature and purposes of the processing, any cost of implementation and any risks to rights and freedoms of data subjects when implementing data processing.

Data Protection Impact Assessment (DPIA)
The school will use a Data Protection Impact Assessment (DPIA) toolkit to evaluate all new computer systems to help it determine how data protection compliance can be assured. In addition, all existing systems will be subject to periodic assessment.

DPIA toolkits provide a step-by-step approach to evaluate and test proposed, new or existing information systems for compliance with the legislation. The DPIA process helps to identify weaknesses or risks to data losses or breaches and to consider action that needs to be taken to ensure compliance where such compliance is not yet achieved. DPIA applies equally to paper as well as electronic data holding systems.

The Data Protection Officer must be consulted when carrying out a DPIA.

Training and awareness
Data Protection training and awareness is crucial so that all staff understand their responsibilities relating to data protection and the use of personal data. Failure to comply with the GDPR and DPA principles could lead to serious problems and, in some cases, may result in significant fines or criminal prosecution.

It is the School's policy that all employees, including managers and Governors, are required to complete the applicable training course annually. This includes employees that do not have internet or email access. Line managers will be responsible for ensuring that staff without internet or email access receive appropriate training.

Role and Responsibilities

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

Head of School
The Head of School acts as the Data Controller on a day-to-day basis.

Data Protection Lead (DPL)

The ICT Network and Systems Manager acts as the Data Protection Lead and is responsible for liaising with the Data Protection Officer and overseeing GDPR and DPA within the school.

Please contact the DPL via email at gdpr@jorichardson.org.uk in the first instance with any questions about the operation of this Data Protection Policy or GDPR or if you have any concerns that this policy is not being or has not been followed.

Data Protection Officer (DPO)

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.

They will provide an annual report of their activities directly to the Governing Body and, where relevant, report to the Governing Body their advice and recommendations on school data protection issues.

Below is our DPO contact information:

Data Protection Officer:	Craig Stilwell
Address:	Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE
Email:	dataservices@judicium.com
Telephone:	0203 326 9174

Policy Review

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed annually. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.