



# General Data Protection Regulation Policy

**Including: Data Protection, Data Retention, Data Breach & Appendix - Subject Access Requests**

<b>Policy Creation &amp; Review</b>	
<b>Author(s)</b>	Sue Ferguson & Judicium
<b>Last review date</b>	September 2019 <i>(amalgamate SAR into this policy)</i>
<b>Ratified by Governing Body</b>	September 2019
<b>Previous Review Dates</b>	June 2018 <i>(compliance with GDPR)</i> February 2017 February 2014
<b>Next Review Date</b>	September 2021

## Introduction

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.

This policy has been created to show how Ellen Wilkinson Primary School & Children's Centre complies with these regulations. For ease of use this has been broken down into the following sections:

- ❖ **Data Protection**
- ❖ **Data Retention**
- ❖ **Data Breach**
- ❖ **Appendix -Subject Access Requests**

### Data Protection Officer (DPO)

The Data Protection Officer is referred to throughout this document, for ease of reference please find below details of the School's Data Protection Officer:

**Data Protection Officer Name:** Craig Stilwell

**Data Protection Officer Details:** Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE

**Data Protection Officer Email:** [dataservices@judicium.com](mailto:dataservices@judicium.com)

**Data Protection Officer Phone:** 020 33269174

# DATA PROTECTION POLICY

## Introduction

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 pupils, parents, suppliers, employees, workers and other third parties.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

## **SECTION 1 - DEFINITIONS**

### **Personal data**

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples 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.

### **Data Subject**

An individual about whom such information is stored is known as the Data Subject. It includes but is not limited to employees.

### **Data Controller**

The organisation storing and controlling such information (i.e. the School) is referred to as the Data Controller.

### **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)**

DPIAs are 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.

## **SECTION 2 - WHEN CAN THE SCHOOL PROCESS PERSONAL DATA**

### **Data Protection Principles**

The School are responsible for and adhere 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 of 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 (i.e. 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 (i.e. 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. Please refer later in this document to the School's Data Retention Policy for further guidance.

**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 safeguard 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 (i.e. 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 process for which it is processed.

The School follow 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. Full details on the School's security measures are set out in the School's E-Safety & Data Security Policy.

**Sharing Personal Data**

The School will generally not share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. These include if the third party: -

- Has a need to know the information for the purposes of providing the contracted services;
- Sharing the personal data complies with the privacy notice that has been provided to the data subject and, if required, the data subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

- The transfer complies with any applicable cross border transfer restrictions; and
- A fully executed written contract that contains GDPR approved third party clauses has been obtained.

There may be circumstances where the School is required either by law or in the best interests of our pupils, parents or staff to pass information onto external authorities, for example, the local authority, Ofsted or the department of health. These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

The intention to share data relating to individuals to an organisation outside of our School shall be clearly defined within written notifications and details and basis for sharing that data given.

### **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.

## **SECTION 3 - DATA SUBJECT'S RIGHTS AND REQUESTS**

Personal data must be made available to data subjects as set out within this policy and data subjects must be allowed to exercise certain rights in relation to their personal data.

The rights data subjects have in relation to how the School handle their personal data are set out below: -

- (a) (Where consent is relied upon as a condition of processing) To withdraw consent to processing at any time;
- (b) Receive certain information about the School's processing activities;
- (c) Request access to their personal data that we hold;
- (d) Prevent our use of their personal data for marketing purposes;
- (e) Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- (f) Restrict processing in specific circumstances;
- (g) Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- (h) Request a copy of an agreement under which personal data is transferred outside of the EEA;
- (i) Object to decisions based solely on automated processing;
- (j) Prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- (k) Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- (l) Make a complaint to the supervisory authority; and
- (m) In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

If any request is made to exercise the rights above, it is a requirement for the relevant staff member within the School to verify the identity of the individual making the request.

### **Subject Access Requests**

A Data Subject has the right to be informed by the School of the following: -

- (a) Confirmation that their data is being processed;

- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;
- (e) The recipients/class of recipients to whom that information is or may be disclosed;
- (f) Details of the School's sources of information obtained;
- (g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct.
- (h) Other supplementary information

Any Data Subject who wishes to obtain the above information must notify the School in writing of his or her request. This is known as a Data Subject Access Request.

The request should in the first instance be sent to the Headteacher (Sue Ferguson).

### **Direct Marketing**

The School are subject to certain rules and privacy laws when marketing. For example a data subject's prior consent will be required for electronic direct marketing (for example, by email, text or automated calls).

The School will explicitly offer individuals the opportunity to object to direct marketing and will do so in an intelligible format which is clear for the individual to understand. The School will promptly respond to any individual objection to direct marketing.

### **Employee Obligations**

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the School in the course of their employment or engagement. If so, the School expects those employees to help meet the School's data protection obligations to those individuals. Specifically, you must: -

- Only access the personal data that you have authority to access, and only for authorised purposes;
- Only allow others to access personal data if they have appropriate authorisation;
- Keep personal data secure (for example by complying with rules on access to school premises, computer access, password protection and secure file storage and destruction (please refer to
- Not to remove personal data or devices containing personal data from the School premises unless appropriate security measures are in place (such as Pseudonymisation, encryption, password protection) to secure the information;
- Not to store personal information on local drives.

### **SECTION 4 - ACCOUNTABILITY**

The School will ensure compliance with data protection principles by implementing appropriate technical and organisational measures. We are responsible for and demonstrate accountability with the GDPR principles.

The School have taken the following steps to ensure and document GDPR compliance: -

#### **Data Protection Officer (DPO)**

Please find below details of the School's Data Protection Officer: -

**Data Protection Officer Name:** Craig Stilwell

**Data Protection Officer Details:** Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE

**Data Protection Officer Email:** [dataservices@judicium.com](mailto:dataservices@judicium.com)

**Data Protection Officer Phone:** 020 33269174



The DPO is responsible for overseeing this data protection policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this Data Protection Policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances: -

- (a) If you are unsure of the lawful basis being relied on by the School to process personal data;
- (b) If you need to rely on consent as a fair reason for processing (please see below the section on consent for further detail);
- (c) If you need to draft privacy notices or fair processing notices;
- (d) If you are unsure about the retention periods for the personal data being processed [although you may find it helpful to refer to the School's data retention policy in the first instance];
- (e) If you are unsure about what security measures need to be put in place to protect personal data;
- (f) If there has been a personal data breach [please see breach notification later in this document];
- (g) If you are unsure on what basis to transfer personal data outside the EEA;
- (h) If you need any assistance dealing with any rights invoked by a data subject;
- (i) Whenever you are engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if you plan to use personal data for purposes other than what it was collected for;
- (j) If you plan to undertake any activities involving automated processing or automated decision making;
- (k) If you need help complying with applicable law when carrying out direct marketing activities;
- (l) If you need help with any contracts or other areas in relation to sharing personal data with third parties.

### **Personal Data Breaches**

The GDPR requires the School to notify any applicable personal data breach to the Information Commissioner's Office (ICO).

We have put in place procedures to deal with any suspected personal data breach 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 person designated as the key point of contact for personal data breaches (who is Sue Ferguson – the Headteacher) or your DPO.

### **Transparency and Privacy Notices**

The School will provide detailed, specific information to data subjects. This information will be provided through the School's privacy notices which are concise, transparent, intelligible, easily accessible and in clear and plain language so that a data subject can easily understand them. Privacy notices sets out information for data subjects about how the School use their data and the School's privacy notices are tailored to suit the data subject.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we will provide the data subject with all the information required by the GDPR including the identity of the data protection officer, the School's contact details, how and why we will use, process, disclose, protect and retain personal data. This is provided in our privacy notices.

When personal data is collected indirectly (for example from a third party or publically available source), we will provide the data subject with the above information as soon as possible after receiving the data. The School will also confirm whether that third party has collected and processed data in accordance with the GDPR.

Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as "children" under the GDPR

### **Privacy by Design**

The School adopt 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 processes.

### **Data Protection Impact Assessments (DPIAs)**

In order to achieve a privacy by design approach, the School conduct DPIAs for any new technologies or programmes being used by the School which could affect the processing of personal data. In any event the School carries out DPIAs when required by the GDPR in the following circumstances: -

- For the use of new technologies (programs, systems or processes) or changing technologies;
- For the use of automated processing;
- For large scale processing of special category data;
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV).

Our DPIAs contain: -

- A description of the processing, its purposes and any legitimate interests used;
- An assessment of the necessity and proportionality of the processing in relation to its purpose;
- An assessment of the risk to individuals; and
- The risk mitigation measures in place and demonstration of compliance.

### **Record Keeping**

The School are required to keep full and accurate records of our data processing activities. These records include: -

- The name and contact details of the School;
- The name and contact details of the Data Protection Officer;
- Descriptions of the types of personal data used;
- Description of the data subjects;
- Details of the School's processing activities and purposes;
- Details of any third party recipients of the personal data;
- Where personal data is stored;
- Retention periods; and
- Security measures in place.

### **Training**

The School will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws.

### **Audit**

The School through its data protection officer regularly test our data systems and processes in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

### **Related Policies**

Staff should refer to the following sections within this GDPR policy: -

- Data retention policy;
- Data breach policy;

And in addition the following separate policies:

- E-Safety & Data Security policy.
- Freedom of Information policy and publication scheme.

These policies are also designed to protect personal data and can be found on our website [www.ellenwilkinson.newham.sch.uk](http://www.ellenwilkinson.newham.sch.uk). Alternatively you can contact main reception who will provide you with a hard copy.

## **SECTION 5 - AUTOMATED PROCESSING AND AUTOMATED DECISION MAKING**

Generally automated decision making is prohibited when a decision has a legal or similar significant effect on an individual unless:

- (a) The data subject has given explicit consent;
- (b) The processing is authorised by law; or
- (c) The processing is necessary for the performance of or entering into a contract.

If certain types of sensitive data are being processed, then (b) or (c) above will not be allowed unless it is necessary for the substantial public interest (for example fraud prevention).

At EWPS we do not use automated processing and decision making.

### **Monitoring**

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

# DATA RETENTION POLICY

The School has a responsibility to maintain its records and record keeping systems. When doing this, the School will take account of the following factors: -

- The most efficient and effective way of storing records and information;
- The confidential nature of the records and information stored;
- The security of the record systems used;
- Privacy and disclosure; and
- Their accessibility.

This policy does not form part of any employee's contract of employment and is not intended to have contractual effect. It does, however, reflect the School's current practice, the requirements of current legislation and best practice and guidance. It may be amended by the School from time to time and any changes will be notified to employees within one month of the date on which the change is intended to take effect. The School may also vary any parts of this procedure, including any time limits, as appropriate in any case.

## DATA PROTECTION

This section sets out how long employment-related and pupil data will normally be held by us and when that information will be confidentially destroyed in compliance with the terms of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.

Data will be stored and processed to allow for the efficient operation of the School. See previous sections for the school's duties and obligations under the GDPR.

## RETENTION SCHEDULE

Information (hard copy and electronic) will be retained for at least the period specified in the attached retention schedule. When managing records, the School will adhere to the standard retention times listed within that schedule.

Paper records will be regularly monitored by Office Manager.

Electronic records will be regularly monitored by the Network Manager & Office Manager.

The schedule is a relatively lengthy document listing the many types of records used by the school and the applicable retention periods for each record type. The retention periods are based on business needs and legal requirements. The retention schedule for EWPS can be found in Appendix 1

## DESTRUCTION OF RECORDS

Where records have been identified for destruction they should be disposed of in an appropriate way. All information must be reviewed before destruction to determine whether there are special factors that mean destruction should be delayed, such as potential litigation, complaints or grievances.

All paper records containing personal information, or sensitive policy information should be shredded before disposal where possible. All other paper records should be disposed of by an appropriate waste paper merchant. All electronic information will be deleted.

The School maintains a database of records which have been destroyed and who authorised their destruction. When destroying documents, the appropriate staff member should record in this list at least: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

## ARCHIVING

Where records have been identified as being worthy of preservation over the longer term, arrangements should be made to transfer the records to the archives. A database of the records sent to the archives is maintained by the

Office Manager. The appropriate staff member, when archiving documents should record in this list the following information: -

- File reference (or other unique identifier);
- File title/description;
- Number of files; and
- Name of the authorising officer.

#### **TRANSFERRING INFORMATION TO OTHER MEDIA**

Where lengthy retention periods have been allocated to records, members of staff may wish to consider converting paper records to other media such as digital media or virtual storage centres (such as cloud storage). The lifespan of the media and the ability to migrate data where necessary should always be considered.

#### **RESPONSIBILITY AND MONITORING**

The Headteacher has primary and day-to-day responsibility for implementing this Policy. The Data Protection Officer, in conjunction with the School is responsible for monitoring its use and effectiveness and dealing with any queries on its interpretation. The data protection officer will consider the suitability and adequacy of this policy and report improvements directly to management.

Internal control systems and procedures will be subject to regular audits to provide assurance that they are effective in creating, maintaining and removing records.

Management at all levels are responsible for ensuring those reporting to them are made aware of and understand this Policy and are given adequate and regular training on it.

# DATA BREACH POLICY

The General Data Protection Regulation (GDPR) 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 GDPR places obligations on staff to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of staff are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to all staff to enable them to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the School of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the School's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the School and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy in order to remain compliant with legal obligations.

## **Definitions**

### **Personal Data**

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples 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'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.

### **Personal Data Breach**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

### **Data Subject**

Person to whom the personal data relates.

### **ICO**

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

## **Responsibility**

The Headteacher has overall responsibility for breach notification within the School. They are responsible for ensuring breach notification processes are adhered to by all staff and are the designated point of contact for personal data breaches.

In the absence of the Headteacher please do contact the Deputy Headteacher (Janice Owen-Amadasun and/or Peter Hilton)

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

The DPO's contact details are set out below: -

**Data Protection Officer Name:** Craig Stilwell

**Data Protection Officer Details:** Judicium Consulting Ltd, 72 Cannon Street, London, EC4N 6AE

**Data Protection Officer Email:** [dataservices@judicium.com](mailto:dataservices@judicium.com)

**Data Protection Officer Phone:** 020 33269174

### **Security and Data-Related Policies**

Staff should refer to the following sections that are related to this data protection policy: -

**Security** - sets out the School's guidelines and processes on keeping personal data secure against loss and misuse.

**Data Protection** - sets out the School's obligations under GDPR about how they process personal data.

### **Data Breach Procedure**

#### **What Is A Personal Data Breach?**

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data or special category data transmitted, stored or otherwise processed.

Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing and other "blagging" attacks where information is obtained by deceiving whoever holds it.

#### **When Does It Need To Be Reported?**

The School must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals then the individuals must also be notified directly.

## **Reporting A Data Breach**

If you know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should:

- Complete a data breach report form (which can be obtained from the main office);
- Email the completed form to the Headteacher (Sue Ferguson)

Where appropriate, you should liaise with your line manager about completion of the data report form. Breach reporting is encouraged throughout the School and staff are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from their line manager, the Headteacher or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular you must not notify any affected individuals or regulators or investigate further. The Headteacher will acknowledge receipt of the data breach report form and take appropriate steps to deal with the report in collaboration with the DPO.

## **Managing and Recording The Breach**

On being notified of a suspected personal data breach, the Headteacher will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so they will take steps to:-

- Where possible, contain the data breach;
- As far as possible, recover, rectify or delete the data that has been lost, damaged or disclosed;
- Assess and record the breach in the School's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

## **Notifying the ICO**

The Headteacher will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of school holidays (i.e. it is not 72 working hours). If the School are unsure of whether to report a breach, the assumption will be to report it.

Where the notification is not made within 72 hours of becoming aware of the breach, written reasons will be recorded as to why there was a delay in referring the matter to the ICO.

## **Notifying Data Subjects**

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Headteacher will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the School have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the Headteacher will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the School will consider alternative means to make those affected aware (for example by making a statement on the School website).

## **Notifying Other Authorities**

The School will need to consider whether other parties need to be notified of the breach. For example: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);



- Local authority;
- The police (for example if the breach involved theft of equipment or data).

This list is non-exhaustive.

### **Assessing The Breach**

Once initial reporting procedures have been carried out, the School will carry out all necessary investigations into the breach.

The School will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction or unauthorised disclosure of personal data. We will identify ways to recover correct or delete data (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the School will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;
- What are the likely consequences of the personal data breach on the school; and
- Any other wider consequences which may be applicable.

### **Preventing Future Breaches**

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether its necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

### **Reporting Data Protection Concerns**

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the Headteacher or the DPO. This can help capture risks as they emerge, protect the School from data breaches and keep our processes up to date and effective.

### **Monitoring**

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the School.

## Appendix A

### SUBJECT ACCESS REQUESTS

Under Data Protection Law, Data Subjects have a general right to find out whether the School hold or process personal data about them, to access that data, and to be given supplementary information. This is known as the right of access, or the right to make a data subject access request (SAR). The purpose of the right is to enable the individual to be aware of, and verify, the lawfulness of the processing of personal data that the School are undertaking.

A Data Subject has the right to be informed by the School of the following: -

- (a) Confirmation that their data is being processed;
- (b) Access to their personal data;
- (c) A description of the information that is being processed;
- (d) The purpose for which the information is being processed;
- (e) The recipients/class of recipients to whom that information is or may be disclosed;
- (f) Details of the School's sources of information obtained;
- (g) In relation to any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct; and
- (h) Other supplementary information.

#### **How to recognise a subject access request**

A data subject access request is a request from an individual (or from someone acting with the authority of an individual, e.g. a solicitor or a parent making a request in relation to information relating to their child):

- for confirmation as to whether the School process personal data about him or her and, if so
- for access to that personal data
- and/or certain other supplementary information

A valid SAR can be both in writing (by letter, email, WhatsApp text) or verbally (e.g. during a telephone conversation). The request may refer to the GDPR and/or to 'data protection' and/or to 'personal data' but does not need to do so in order to be a valid request. For example, a letter which states 'please provide me with a copy of information that the School hold about me' will be a data subject access request and should be treated as such. Alternatively the form in Appendix B can be used.

A data subject is generally only entitled to access their own personal data, and not information relating to other people.

#### **How to make a data subject access request**

Whilst there is no requirement to do so, we encourage any individuals who wish to make such a request to make the request in writing, detailing exactly the personal data being requested. This allows the School to easily recognise that you wish to make a data subject access request and the nature of your request. If the request is unclear/ vague we may be required to clarify the scope of the request which may in turn delay the start of the time period for dealing with the request.

#### **What to do when you receive a data subject access request**

All data subject access requests should be immediately directed to the Headteacher who should contact Judicium as DPO in order to assist with the request and what is required.

#### **Acknowledging the request**

When receiving a SAR the School shall acknowledge the request as soon as possible and inform the requester about the statutory deadline (of one calendar month) to respond to the request.

In addition to acknowledging the request, the School may ask for:

- proof of ID (if needed);
- further clarification about the requested information;
- if it is not clear where the information shall be sent, the School must clarify what address/email address to use when sending the requested information; and/or
- consent (if requesting third party data).

The School should work with their DPO in order to create the acknowledgment.

#### **Verifying the identity of a requester or requesting clarification of the request**

Before responding to a SAR, the School will take reasonable steps to verify the identity of the person making the request. In the case of current employees, this will usually be straightforward. The School is entitled to request additional information from a requester in order to verify whether the requester is in fact who they say they are. Where the School has reasonable doubts as to the identity of the individual making the request, evidence of identity may be established by production of a passport, driving license, a recent utility bill with current address, birth/marriage certificate, credit card or a mortgage statement.

If an individual is requesting a large amount of data the School may ask the requester for more information for the purpose of clarifying the request, but the requester shall never be asked why the request has been made. The School shall let the requestor know as soon as possible where more information is needed before responding to the request.

In both cases, the period of responding begins when the additional information has been received. If the School do not receive this information, they will be unable to comply with the request.

#### **Requests made by third parties or on behalf of children**

The school need to be satisfied that the third party making the request is entitled to act on behalf of the individual, but it is the third party's responsibility to provide evidence of this entitlement. This might be a written authority to make the request or it might be a more general power of attorney. The School may also require proof of identity in certain circumstances.

When requests are made on behalf of children, it is important to note that even if a child is too young to understand the implications of subject access rights, it is still the right of the child, rather than of anyone else such as a parent or guardian, to have access to the child's personal data. Before responding to a SAR for information held about a child, the School should consider whether the child is mature enough to understand their rights. If the school is confident that the child can understand their rights, then the School should usually respond directly to the child or seek their consent before releasing their information.

It shall be assessed if the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so. When considering borderline cases, it should be taken into account, among other things:

- the child's level of maturity and their ability to make decisions like this;
- the nature of the personal data;
- any court orders relating to parental access or responsibility that may apply;
- any duty of confidence owed to the child or young person;
- any consequences of allowing those with parental responsibility access to the child's or young person's information. This is particularly important if there have been allegations of abuse or ill treatment;
- any detriment to the child or young person if individuals with parental responsibility cannot access this information; and
- any views the child or young person has on whether their parents should have access to information about them.

Generally, a person aged 12 years or over is presumed to be of sufficient age and maturity to be able to exercise their right of access, unless the contrary is shown. In relation to a child 12 years of age or older, then provided that the School is confident that they understand their rights, and there is no reason to believe that the child does not have the capacity to make a request on their own behalf, the School will require the written authorisation of the child before responding to the requester, or provide the personal data directly to the child.

The School may also refuse to provide information to parents if there are consequences of allowing access to the child's information – for example if it is likely to cause detriment to the child.

### **Fee for responding to a SAR**

The School will usually deal with a SAR free of charge. Where a request is considered to be manifestly unfounded or excessive a fee to cover administrative costs may be requested.

### **Time Period for Responding to a SAR**

The School has one calendar month to respond to a SAR. This will run from the day that the request was received or from the day when any additional identification or other information requested is received, or payment of any required fee has been received.

The period for response may be extended by a further two calendar months in relation to complex requests. What constitutes a complex request will depend on the particular nature of the request. The DPO must always be consulted in determining whether a request is sufficiently complex as to extend the response period.

Where a request is considered to be sufficiently complex as to require an extension of the period for response, the School will need to notify the requester within one calendar month of receiving the request, together with reasons as to why this extension is considered necessary.

### **School closure periods**

Requests received during or just before school closure periods may not be able to be responded to within the one calendar month response period. This is because the School will be closed, our mail gets forwarded and we do not review emails during this period. As a result, it is unlikely that your request will be able to be dealt with during this time. We may not be able to acknowledge your request during this time (i.e. until a time when we receive the request), however, if we can acknowledge the request we may still not be able to deal with it until the School re-opens. The School will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during/close to closure periods.

### **Information to be provided in response to a request**

The individual is entitled to receive access to the personal data we process about him or her.

The information should be provided in a way that is concise, transparent, easy to understand and easy to access using clear and plain language, with any technical terms, abbreviations or codes explained. The response shall be given in writing if the SAR was made in writing in a commonly-used electronic format.

The information that the School are required to supply in response to a SAR must be supplied by reference to the data in question at the time the request was received. However, as the School have one month in which to respond the School is allowed to take into account any amendment or deletion made to the personal data between the time the request is received and the time the personal data is supplied if such amendment or deletion would have been made regardless of the receipt of the SAR.

The School is therefore, allowed to carry out regular housekeeping activities even if this means deleting or amending personal data after the receipt of a SAR. The School is not allowed to amend or delete data to avoid supplying the data.

### **How to locate information**

The personal data the School need to provide in response to a data subject access request may be located in several of the electronic and manual filing systems. This is why it is important to identify at the outset the type of information requested so that the search can be focused.

### **Protection of third parties -exemptions to the right of subject access**

There are circumstances where information can be withheld pursuant to a SAR. These specific exemptions and requests should be considered on a case by case basis.

The School will consider whether it is possible to redact information so that this does not identify those third parties. If their data cannot be redacted (for example, after redaction it is still obvious who the data relates to) then the School do not have to disclose personal data to the extent that doing so would involve disclosing information relating to another individual (including information identifying the other individual as the source of information) who can be identified from the information unless:

- the other individual has consented to the disclosure; or

- it is reasonable to comply with the request without that individual's consent.

In determining whether it is reasonable to disclose the information without the individuals consent, all of the relevant circumstances will be taken into account, including:

- the type of information that they would disclose;
- any duty of confidentiality they owe to the other individual;
- any steps taken to seek consent from the other individual;
- whether the other individual is capable of giving consent; and
- any express refusal of consent by the other individual.

It needs to be decided whether it is appropriate to disclose the information in each case. This decision will involve balancing the data subject's right of access against the other individual's rights. If the other person consents to the school disclosing the information about them, then it would be unreasonable not to do so. However, if there is no such consent, the school must decide whether to disclose the information anyway. If there are any concerns in this regard then the DPO should be consulted.

### **Other exemptions to the right of subject access**

In certain circumstances the School may be exempt from providing some or all of the personal data requested. These exemptions are described below and should only be applied on a case-by-case basis after a careful consideration of all the facts.

**Crime detection and prevention:** The School do not have to disclose any personal data being processed for the purposes of preventing or detecting crime; apprehending or prosecuting offenders; or assessing or collecting any tax or duty.

**Confidential references:** The School do not have to disclose any confidential references given to third parties for the purpose of actual or prospective:

- education, training or employment of the individual;
- appointment of the individual to any office; or
- provision by the individual of any service

This exemption does not apply to confidential references that the School receive from third parties. However, in this situation, granting access to the reference may disclose the personal data of another individual (i.e. the person giving the reference), which means that the School must consider the rules regarding disclosure of third-party data set out above before disclosing the reference.

**Legal professional privilege:** The School do not have to disclose any personal data which are subject to legal professional privilege.

**Management forecasting:** The School do not have to disclose any personal data processed for the purposes of management forecasting or management planning to assist us in the conduct of any business or any other activity.

**Negotiations:** The School do not have to disclose any personal data consisting of records of intentions in relation to any negotiations with the individual where doing so would be likely to prejudice those negotiations.

## Appendix B

### Subject Access Request Form

The Data Protection Act 2018 provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Please complete this form if you wish to make a request for your data. Your request will normally be processed within one calendar month upon receipt of a fully completed form and proof of identity.

**Proof of identity:** We require proof of your identity before we can disclose personal data. Proof of your identity should include a copy of a document such as your birth certificate, passport, driving licence, official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill. The document should include your name, date of birth and current address. If you have changed your name, please supply relevant documents evidencing the change.

#### Section 1

Please fill in the details of the data subject (i.e. the person whose data you are requesting). If you are not the data subject and you are applying on behalf of someone else, please fill in the details of the data subject below and not your own.

Title	
Surname/Family Name	
First Name(s)/ Forename	
Date of Birth	
Address	
Post Code	
Phone Number	
Email address	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- Birth Certificate
- Driving Licence
- Passport
- An official letter to my address

#### **Personal Information**

*If you only want to know what information is held in specific records, please indicate in the box below. Please tell us if you know in which capacity the information is being held, together with any names or dates you may have. If you do not know exact dates, please give the year(s) that you think may be relevant.*

**Details:**

**Employment records:**

If you are, or have been employed by the School and are seeking personal information in relation to your employment please provide details of your Staff number/Unit/Team/Dates of employment.

**Details:**

**Section 2**

Please complete this section of the form with your details if you are acting on behalf of someone else (i.e. the data subject).

If you are **NOT** the data subject, but an agent appointed on their behalf, you will need to provide evidence of your identity as well as that of the data subject and proof of your right to act on their behalf.

Title	
Surname/ Family Name	
First Name(s)/Forenames	
Date of Birth	
Address	
Post Code	
Phone Number	

I am enclosing the following copies as proof of identity (please tick the relevant box):

- Birth Certificate
- Driving Licence
- Passport
- An official letter to my address

**What is your relationship to the data subject?** (e.g. parent, carer, legal representative)

I am enclosing the following copy as proof of legal authorisation to act on behalf of the data subject:

- Letter of authority
- Lasting or Enduring Power of Attorney
- Evidence of parental responsibility
- Other (give details):

### Section 3

Please describe as detailed as possible what data you request access to (time period/ categories of data/ information relating to a specific case/ paper records/ electronic records).

I wish to:

- Receive the information by post\*
- Receive the information by email
- Collect the information in person
- View a copy of the information only
- Go through the information with a member of staff

\*Please be aware that if you wish us to post the information to you, we will take every care to ensure that it is addressed correctly. However, we cannot be held liable if the information is lost in the post or incorrectly delivered or opened by someone else in your household. Loss or incorrect delivery may cause you embarrassment or harm if the information is 'sensitive'.

**Please send your completed form and proof of identity by email to: [info@ellenwilkinson.newham.sch.uk](mailto:info@ellenwilkinson.newham.sch.uk)**