

# Data Protection Policy

## Gwladys Street CP & Nursery School



Based on the Liverpool City Council  
Model Data Protection Act 2018 Policy for Schools

Approved by:

Date: February 2019

Last reviewed on: [N/A]

Next review due by: Summer 2019

## Contents

1. Aims.....	2
2. Legislation and guidance .....	3
3. Definitions .....	3
4. The data controller .....	4
5. Roles and responsibilities .....	5
6. Data protection principles.....	5
7. Collecting personal data.....	6
8. Sharing personal data .....	7
9. Subject access requests and other rights of individuals .....	8
10. Parental requests to see the educational record .....	9
11. CCTV .....	9
13. Photographs and videos .....	10
14. Data protection by design and default .....	10
15. Data security and storage of records.....	10
16. Storage and retention of personal information.....	11
17. Personal data breaches .....	12
18. Training.....	12
19. Consequences of a failure to comply .....	12
20. Links with other policies .....	12
21. Glossary.....	14
Appendix 1: Personal data breach procedure .....	16
Appendix 2 – Procedure for Access to Personal Information.....	18

---

### 1. Aims

General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) is the law that protects personal privacy and upholds individual’s rights. It applies to anyone who handles or has access to people’s personal data.

Our school aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the [General Data Protection Regulation \(GDPR\)](#) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the [Data Protection Bill](#).

The school is committed to being concise, clear and transparent about how it obtains and uses personal information and will ensure data subjects are aware of their rights under the legislation.

All staff and volunteers must have a general understanding of the law and understand how it may affect their decisions in order to make an informed judgement about how information is gathered, used and ultimately deleted. All staff must read, understand and comply with this policy.

The Information Commissioner as the Regulator can impose fines of up to 20 million Euros (approximately £17 million) for serious breaches of the GDPR, therefore it is imperative that the School and all staff and volunteers comply with the legislation.

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

## Scope of the Policy

Personal data is any information that relates to an identified or identifiable living individual who can be identified directly or indirectly from the information. The information includes factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a living individual. This includes any expression of opinion about an individual and intentions towards an individual. Under the Data Protection Act 2018 personal information also includes an identifier such as a name, an identification number, location data or an online identifier.

The School collects a large amount of personal data every year including: pupil records, staff records, names and addresses of those requesting prospectuses, examination marks, references, fee collection as well as the many different types of research data used by the School. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities (LAs), government agencies and other bodies.

## 2. Legislation and guidance

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

It also reflects the ICO's [code of practice](#) for the use of surveillance cameras and personal information.

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

## 3. Definitions

Term	Definition
<b>Personal data</b>	Any information relating to an identified, or identifiable, individual. <sup>1</sup>  This may include the individual's: <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li></ul>

---

<sup>1</sup> GDPR Article 4 Definitions

	<ul style="list-style-type: none"> <li>• Location data</li> <li>• Online identifier, such as a username</li> </ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>
<b>Special categories of personal data</b>	<p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> <li>• Racial or ethnic origin</li> <li>• Political opinions</li> <li>• Religious or philosophical beliefs</li> <li>• Trade union membership</li> <li>• Genetics</li> <li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li> <li>• Health – physical or mental</li> <li>• Sex life or sexual orientation</li> </ul>
<b>Processing</b>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying.</p> <p>Processing can be automated or manual.</p>
<b>Data subject</b>	<p>The identified or identifiable individual whose personal data is held or processed.</p>
<b>Data controller</b>	<p>A person or organisation that determines the purposes and the means of processing of personal data.</p>
<b>Data processor</b>	<p>A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.</p>
<b>Personal data breach</b>	<p>A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.</p>

#### 4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The school is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

## 5. Roles and responsibilities

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

### 5.1 Governing board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations.

### 5.2 Data protection officer

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will report to the board their advice and recommendations on school data protection issues.

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

Our DPO is Chris Walsh and is contactable via T: 0151 233 0410 / [chris.walsh@liverpool.gov.uk](mailto:chris.walsh@liverpool.gov.uk)

### 5.3 Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

### 5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
  - If there has been a data breach
  - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
  - If they need help with any contracts or sharing personal data with third parties

## 6. Data protection principles

The GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure and protects against unauthorized or unlawful processing of personal data, accidental loss or destruction of, or damage to personal data

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

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

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

- The data needs to be processed so that the school can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the school, as a public authority, can perform a task **in the public interest**, and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the school or a third party<sup>2</sup> (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear **consent**

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

If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get general parental consent (except for online counselling and preventive services).

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

### Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited<sup>3</sup> unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

Sensitive personal information will only be processed if:

- There is a lawful basis for doing so as identified on previous page
- One of the special conditions for processing sensitive personal information applies:
  - a. the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
  - b. the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject

---

<sup>2</sup> The GDPR states that legitimate interests do not apply to processing carried out by public authorities in the performance of their tasks, Article 6 However, the ICO indicates that where there are other legitimate purposes outside the scope of the tasks as a public authority, legitimate interests may be considered where appropriate (particularly relevant for public authorities with commercial interests).

<sup>3</sup> GDPR, Article 9

- c. the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
- d. the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
- e. the processing relates to personal data which are manifestly made public by the data subject
- f. the processing is necessary for the establishment, exercise or defence of legal claims
- g. the processing is necessary for reasons of substantial public interest
- h. the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
- i. the processing is necessary for reasons of public interest in the area of public health.

The school's privacy notice(s) set out the types of sensitive personal information that it processes, what it is used for, the lawful basis for the processing and the special condition that applies.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

Unless the School can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data. Evidence of consent will need to be captured and recorded so that the school can demonstrate compliance with the Data Protection Act 2018.

## 7.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the [Information and Records Management Society's toolkit for schools](#)

## 8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk
- We need to liaise with 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.

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

## **9. Subject access requests and other rights of individuals**

### **9.1 Subject access requests**

Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

Subject access requests should include:

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

If staff receive a subject access request they must immediately forward it to the DPO.

### **9.2 Children and subject access requests**

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our school may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

### **9.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge



- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

#### **9.4 Other data protection rights of the individual**

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

## **10. Parental requests to see the educational record**

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

## **11. 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.

Any enquiries about the CCTV system should be directed to Miss N. Booth, (the headteacher).

## 13. Photographs and videos

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

*All schools add and adapt to reflect your school's uses of photographs and videos for communication, marketing and promotional materials:*

Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns, sports competitions etc
- Online on our school website or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

## 14. Data protection by design and default

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices)
  - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

## 15. Data security and storage of records

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy.

The school will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). It will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

Staff must maintain data security by protecting the **confidentiality, integrity and availability** of the personal data, defined as follows:

**Confidentiality** means that only people who have a need to know and are authorised to use the personal data can access it.

**Integrity** means that personal data is accurate and suitable for the purpose for which it is processed.

**Availability** means that authorised users can access the personal data when they need it for authorised purposes.

Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the school has implemented and maintains in accordance with the GDPR and DPA.

Where the school uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

- the organisation may only act on the written instructions of the school
- those processing data are subject to the duty of confidence
- appropriate measures are taken to ensure the security of processing
- sub-contractors are only engaged with the prior consent of the school and under a written contract
- the organisation will assist the school in providing subject access and allowing individuals to exercise their rights in relation to data protection
- the organisation will delete or return all personal information to the school as requested at the end of the contract
- the organisation will submit to audits and inspections, provide the school with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the school immediately if it does something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval from the DPO.

## 16. Storage and retention of personal information

Personal data will be kept securely in accordance with the school's data protection obligations.

Personal data should not be retained for any longer than necessary. The length of time data should be retained will depend upon the circumstances, including the reasons why personal data was obtained. Staff should adhere to the LCC Schools Retention Schedule on Ed-net.

Personal information that is no longer required will be deleted in accordance with the Schools Record Retention Schedule.

## 17. Personal data breaches

The school will make all reasonable endeavours to ensure that there are no personal data breaches. A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff and volunteers should ensure they inform their line manager/DPO/Head teacher immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

## 18. Training

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

## 19. Consequences of a failure to comply

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO. Your schools DPO is Chris Walsh who can be contacted on 233-0410 or [chris.walsh@liverpool.gov.uk](mailto:chris.walsh@liverpool.gov.uk)

## 20. Links with other policies

This data protection policy is linked to our:

- Online Safety Policy,
- Acceptable Use of ICT Agreements
- Child Protection Policy

- Complaints Procedure Policy
- Computing Policy

### **Review of Policy**

This policy will be updated as necessary to reflect best practice or amendments made to the DPA 2018.

### **The Supervisory Authority in the UK**

Please follow this link to the ICO's website (<https://ico.org.uk/>) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.

## 21. Glossary

**Automated Decision-Making (ADM):** when a decision is made which is based solely on automated processing (including profiling) which produces legal effects or significantly affects an individual. The Data Protection Act 2018 prohibits automated decision-making (unless certain conditions are met) but not automated processing.

**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. profiling is an example of automated processing.

**Consent:** agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, which signifies agreement to the processing of personal data relating to them.

**Data Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. It is responsible for establishing practices and policies in line with the Data Protection Act 2018. The school is the Data Controller of all personal data relating to its pupils, parents and staff.

**Data Subject:** a living, identified or identifiable individual about whom we hold personal data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

**Data Privacy Impact Assessment (DPIA):** tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major systems or business change programs involving the processing of personal data.

**Data Protection Officer (DPO):** the person required to be appointed in public authorities under the GDPR.

**EEA:** the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

**Explicit Consent:** consent which requires a very clear and specific statement (not just action).

**General Data Protection Regulation (GDPR):** General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

**Personal data** is any information relating to an identified or identifiable natural person (data subject) who can be identified, directly or indirectly by reference to an identifier such as a name, 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 includes sensitive personal 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 example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

**Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Privacy by Design:** implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

**Privacy Notices:** separate notices setting out information that may be provided to Data Subjects when the school collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, school workforce privacy policy) or they may be stand-alone privacy statements covering processing related to a specific purpose.

**Processing** means anything done with personal data, such as collection, recording, structuring, storage, adaptation or alteration, retrieval, use, disclosure, dissemination or otherwise making available, restriction, erasure or destruction.

**Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller.

**Pseudonymisation or Pseudonymised:** replacing 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.

**Sensitive Personal Data:** information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal data relating to criminal offences and convictions.

## Appendix 1: Personal data breach procedure

This procedure is based on [guidance on personal data breaches](#) produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people
- The DPO will alert the headteacher and the chair of governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

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

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored [on the school's computer system](#).
- Where the ICO must be notified, the DPO will do this via the ['report a breach' page of the ICO website](#) within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible



- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

Records of all breaches will be stored **on the school's computer system**.

The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

### **Actions to minimise the impact of data breaches**

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

#### ***Sensitive information being disclosed via email (including safeguarding records)***

- *If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error*
- *Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error*
- *If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to recall it*
- *In any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request*
- *The DPO will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted*

#### ***Sensitive information be disclosed via electronic devices***

- *Electronic devices carrying sensitive personal data shall be encrypted.*
- *If a school laptop containing non-encrypted sensitive personal data is stolen or hacked the DPO and headteacher will be informed immediately and necessary steps will be taken to try and retrieve the data (e.g. inform the police) The DPO will be informed immediately and a decision made as to whether to inform the ICO.*

## Appendix 2 – Procedure for Access to Personal Information

### Gwladys Street CP & Nursery School

#### 1. Right of access to information

There are two distinct rights of access to personal information held by schools.

**Under the GDPR and the Data Protection Act 2018** an individual (e.g. pupil, parent or member of staff) has a right to request access to their own personal information. In certain circumstances requests may be made by a parent on behalf of their child (see explanation below).

**The Education (Pupil Information) (England) Regulations 2005** gives parents the right of access to curricular and educational records relating to their child.

#### 2. Processing a request

Requests for personal information must be made in writing and addressed to the Headteacher. If the initial request does not clearly identify the information required, then clarification should be sought.

The identity of the requestor must be verified before the disclosure of any personal information, and checks should also be carried out regarding proof of relationship to the child.

Evidence of identity can be established by requesting production of the following (this list is not exhaustive):

- passport
- driving licence
- utility bills with the current address
- Birth / Marriage certificate
- P45/P60
- Credit Card or Mortgage statement
- Parental Responsibility

Individuals are entitled to be told if we are processing their personal information, obtain a copy of that information and other supplementary information – see below.

In addition to a copy of their personal data, you also have to provide individuals with the following information:

- the purposes for processing their data;
- the categories of personal data concerned;
- the recipients or categories of recipient you disclose the personal data to;
- your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- the existence of their right to request rectification, erasure or restriction or to object to such processing;
- the right to lodge a complaint with the ICO or another supervisory authority;
- information about the source of the data, where it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards you provide if you transfer personal data to a third country or international organisation.

Much of this information will already be included in your privacy notice.

Information can be viewed at the school with a member of staff on hand to help and explain matters if requested or provided at a face to face handover.

The views of the applicant should be taken into account when considering the method of delivery. If the applicant has asked for the information to be posted then special next day delivery or recorded delivery postal service must be used.

## 2. Information relating to children

Children have the same rights of access to their own personal information as adults, and the same rights of privacy. There is no minimum age in English law, however current practice accepts that, provided a child is mature enough to understand their rights, a child of, or over the age of 12 years shall be considered capable of giving consent. This does not rule out receipt of a valid request from a child of a younger age, as each request should be considered on its merits on an individual basis.

When a subject access request is received from a child it will need to be judged whether the child has the capacity to understand the implications of their request and of the information provided as a result of that request. If the child does understand then their request will be dealt with in the same way as that of an adult.

If a parent or legal guardian makes a request on behalf of a child age 12 and over the request will only be complied with when assurances are received that the child has authorised the request and that their consent was not obtained under duress or on the basis of misleading information. If the child does not understand, then a request from a parent or legal guardian for the child's information will only be complied with when assurances are received that they are acting in the best interests of the child.

For children Accessing internet services where consent is required the age is 13 years and above

## 4. Response time

### GDPR & DPA

The response time for compliance with a subject access request is **one month** following date of receipt. The timeframe does not begin until the school has received all the information necessary to comply with the request i.e. proof of identity.

You may be able to extend the timeframe by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.

## Education Regulations

Requests for information from parents for access to information classed as being part of the education record must be responded to within **15 school days**.

## 5. Charges

### Under GDPR & DPA:

Should the information requested be personal information that **does not** include any information contained within educational records the school cannot make a charge, unless the request is

manifestly unfounded or excessive. You may charge a “reasonable fee” for the administrative costs of complying with the request.

The School can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies.

### **Under the Education Regulations**

The school may make a charge if the information requested relates to the educational record, the amount charged will depend upon the number of pages provided. The fees work on a sliding scale basis as below.

<b>Number of pages</b>	<b>Maximum fee</b>
1-19	£1
20-29	£2
30-39	£3
40-49	£4
50-59	£5
60-69	£6
70-79	£7
80-89	£8
90-99	£9
100-149	£10
150-199	£15
200-249	£20
250-299	£25
300-349	£30
350-399	£35
400-449	£40
450-499	£45
500+	£50

### **6. Exemptions**

There are some exemptions to the right to subject access that apply in certain circumstances or to certain types of personal information. **This means all information must be reviewed prior to disclosure.**

Included below are some of the exemptions that apply to a school, this is not an exhaustive list;

**Third Party information:** If the information held identifies other people, then it will sometimes be right to remove or edit that information so as not to reveal the identity of the third parties, unless the third parties have agreed to the disclosure. (This is less likely to apply to information identifying teachers or other professionals unless to disclose it would cause them serious harm.) Reasonable steps must be taken to obtain third party consent to disclosure. If the third parties cannot be located or do not respond it may still be reasonable to consider disclosure if the information is of importance to the data subject. The school must still adhere to the **one month** statutory timescale.

Where redaction (information edited/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

Information disclosed should be clear, meaning any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

**Information likely to cause serious harm or distress:** Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual involved should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

**Crime and Disorder:** If the disclosure of the information is likely to hinder the prevention or detection of a crime, the prosecution or apprehension of offenders, or the assessment or collection of any tax or duty, the information should be withheld.

**Legal professional privilege:** If the information is general legal advice or advice which relates to anticipated or pending legal proceedings it is subject to 'legal professional privilege'. The disclosure of any communication to or from a legal advisor to another person (including the data subject) should not take place unless this has first been discussed with the legal advisor concerned.

**References:** The right of access does not apply to references given (or to be given) in confidence.

**Absence of or invalid consent to disclosure:** If the data subject is considered incapable of giving valid consent to disclosure (i.e. they do not have the capacity to understand the nature/implications of the access request), or if it is suspected that the consent was obtained under duress by someone acting on their behalf, or based on misleading information, then access should be refused.

## **7. Complaints**

Complaints about the above procedures should be made to the Data Protection Officer (DPO) who will decide whether it is appropriate for the complaint to be dealt with in accordance with the school's complaint procedure.

Complaints which are not appropriate to be dealt with through the school's complaint procedure can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

## **8. Contacts**

If you have any queries or concerns regarding individuals right of access to their own personal information, please contact:

The Information Team  
6<sup>th</sup> Floor  
Cunard Building  
Water Street  
L3 1AH  
Email: [chris.walsh@liverpool.gov.uk](mailto:chris.walsh@liverpool.gov.uk)  
Or [dpo@Liverpool.gov.uk](mailto:dpo@Liverpool.gov.uk)

Further advice and information can be obtained from the Information Commissioner's Office:  
[www.ico.gov.uk](http://www.ico.gov.uk)