Curzon Crescent & Fawood Children's Centres Partnership

Data Protection Policy (incl. Data Breach, SAR, Retention)

Reviewed	**–**	**Autumn 2020**
Next Review	**–**	**Autumn 2021**

Policy Lead – Data Protection Lead

Approving Committee - Resources

Approved by the Governing Board on: ……

Signature of Chair: ……

Document content:

Overview

This policy is drafted in accordance with the requirements of the General Data Protection Regulation ("GDPR"), 25th May 2018, and it covers Curzon Crescent and Fawood Nursery School Children's Centre Partnership1 (referred to as the Partnership within this document)

The objective of the policy is to ensure that The Partnership acts within the requirements of the General Data Protection Regulations May 2018 when retaining and storing personal data and when making it available to individuals. The policy applies to all personal information, no matter how it is collected, used or recorded and covers information held on paper or electronically.

GDPR: General Data Protection Regulation

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR refers to sensitive personal data as 'special categories of personal data'. Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. For example, information about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life or sexual orientation, are all 'special categories of personal data'.

The GDPR applies to 'controllers' and 'processors'. The school is a data controller who determines the purposes and means of processing personal data. A processor is responsible for processing personal data on behalf of the school.

The GDPR gives individuals the right to know what information is held about them. It provides a framework to ensure that personal information is handled properly.

The Act states that anyone who processes personal information must comply with eight principles, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for specific and lawful purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with the individual's rights
- Processed securely
- Not transferred to other countries without adequate protection

Curzon Crescent Children's Centre and Fawood Children's Centre are separately registered as Data Controllers with the Information Commissioner's Office (ICO). The registration numbers are ZA077835 and ZA077833 for Fawood and Curzon Crescent respectively and the registration details can be found on the ICO Website.

Please note - our Data Protection Officer is Deepti Bal – email DPO.Bal@bsp.london

Data Protection

1. Data Protection Principles

Under Article 5(1) of the GDPR, the data protection principles set out the main responsibilities for organisations. It states personal data shall be:

- Anyone **processing personal data** must comply with the data protection principles. These provide that **personal data** must be:
- **Processed** fairly and lawfully and transparently in relation to the **data subject**;
- **Processed** for specified, lawful purposes and in a way which is not incompatible with those purposes;
- Adequate, relevant and not excessive for the purpose;
- Accurate and up to date;
- Not kept for any longer than is necessary for the purpose; and
- **Processed** securely using appropriate technical and organisational measures.
- **Personal Data** must also:
- be **processed** in line with **data subjects'** rights;
- not be transferred to people or organisations situated in other countries without adequate protection.
- We will comply with these principles in relation to any **personal data** we process

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

2. Lawful Processing

The first principle requires that organisations process personal data in a lawful manner. The school/nursery will only process personal data if it can meet one of the following lawful bases set out under Article 6(1):

- Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In addition, if the school/nursery wishes to process 'special category data', it will identify an additional condition for processing as set out under Article 9(2).

3. Consent

Where a need exists to request and receive consent of an individual prior to the collection, use or disclosure of personal data, the school is committed to seeking such consent. In all cases consent must be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's wishes. The Partnership is therefore committed to obtaining consent in the following manner:

- consent is presented in a manner clearly distinguishable from other matters
- the request is made in an intelligible and easily accessible form using plain language

When children and/or a member of staff joins the Partnership they will need to complete a consent form. This consent form deals with the taking and use of photographs and videos of them, amongst other things.

Inform the data subject of exactly what we intend to do with their personal data;

Inform the data subject of how they can withdraw their consent.

- is freely given (i.e. not based on the need to conduct another processing activity)
- the date, method, validity and content of the consent is documented
- a simple method is provided for the data subject to be able to withdraw consent at any time

Any consent must be freely given, which means that we cannot make the provision of any goods or services or other matter conditional on a data subject giving their consent.

The DPO must always be consulted in relation to any consent form before consent is obtained.

A record must always be kept of any consent, including how it was obtained and when.

4. Data Protection Officer (DPO)

Under the GDPR it is mandatory for Local Authorities (as defined by the FOIA) to designate a Data Protection Officer (DPO). The DPO's minimum tasks are defined in Article 39:

Our Data Protection Officer is Deepti Bal who can be contacted via DPO.Bal@bsp.london.

The Partnership has an onsite Data Protection Lead Fiona Gaughan and Deputy Data Protection Lead Jainee Shah.

- To inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff and conduct internal audits
- To be the first point of contact for the Information Commissioner's Office
- The DPO is responsible for ensuring compliance with the Data Protection Legislation and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the DPO.
- The DPO is also the central point of contact for all data subjects and others in relation to matters of data protection.

5. Workforce Training

The Partnership is committed to providing data protection training to all staff and will issue regular refresh training throughout the course of their employment or in the event of any changes in data protection law.

6. Data Protection Impact Assessments (DPIA's)

Data protection impact assessments (DPIAs) are a tool which can help the school identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. An effective DPIA allows organisations to identify and fix problems at an early stage, reducing the associated costs and damage to reputation which might otherwise occur.

The Partnership will complete a DPIA for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. Therefore, staff must consult the relevant persons or DPO before they embark on any new processing that could be regarded as being high risk to an individuals' interests.

Data Breach

The Partnership is committed to the protection of all personal data and special category personal data for which we are the data controller. The law imposes significant fines for failing to lawfully process and safeguard personal data and failure to comply with this policy may result in those fines being applied. All members of our workforce must comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary or other action.

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This could be the result of a breach of cyber security, such as a hack or virus, or it could be the result of a breach of physical security such as loss or theft of a mobile device or paper records. A data breach includes loss of data and so does not have to be the result of a conscious effort of a third party to access the data. Some examples of potential data breaches are listed below:

- Leaving information on a child on the bus or train;
- Theft of a bag containing paper documents;
- Destruction of the only copy of a document; and
- Sending an email or attachment to the wrong recipient; and
- Using an unauthorised email address to access personal data; and
- Leaving paper documents containing personal data in a place accessible to other people.

Reporting a data breach upon discovery

If any member of our workforce suspects, or becomes aware, that a data breach may have occurred (either by them, another member of our workforce, a data processor, or any other individual) then they must immediately contact either the Data Protction Lead (DPL), Deputy DPL or Executive HT or our Data Protection Officer (DPO) via DPO.Bal@bsp.london.

It is a staff member's obligation to report as soon as they become aware of a potential breach (or where there is a suspected breach) so that the Partnership can comply with statutory obligations. This may fall outside of working hours, holidays etc. If a breach occurs out of hours or they are unable to contact staff responsible for GDPR in person, staff should email the relevant staff members listed or DPO immediately and not the next working day. Members of our workforce who fail to report a suspected data breach could face disciplinary or other action.

Contact details:

DPL Fiona Gaughan- Fiona@fawoodcc.brent.sch.uk

D-DPL Jainee Shan – Jainee@fawoodcc.brent.sch.uk

Executive Headteacher – Nisha@curzon.brent.sch.uk

The data breach may need to be reported to the ICO, and notified to data subjects. This will depend on the risk to data subjects. The DPO must always be consulted in making the decision as to whether to report a data breach to the ICO. Initial investigations will inform as to whether the data breach should be reported.

If it is considered to be necessary to report a data breach to the ICO then the school must do so within 72 hours of discovery of the breach. The school may also be contractually required to notify other organisations of the breach within a period following discovery.

Producing an ICO Breach Notification Report

All members of our workforce are responsible for sharing all information relating to a data breach with the DPO, which will enable the annexed Breach Notification Report Form to be completed.

Subject Access Request

What is personal data?

For information to be personal data, it must relate to a living individual and allow that individual to be identified from that information (either on its own or in conjunction with other information held alongside it). The individual to whom the personal data relates to is the 'Data Subject'.

Staff should be aware that requests for any personal data constitute a Subject Access request. Whilst requests can be made and will be accepted verbally, staff should ask requestors to complete the relevant template where possible or alternatively otherwise inform the Admin team of the verbal request, so that the request can be managed within the requirements of the Regulation. If staff are unsure regarding any requests for personal information, they should contact the Data Protection Lead as soon as possible.

A Subject Access Request can be made by

- any parent/carer acting on behalf of their child(ren) as the Data Subject or
- any parent/carer acting in their own individual right as the Data Subject or
- any member of staff as the Data Subject

to find out what personal information is held about them.

How to make a Subject Access Request (SAR)

A request can be submitted to Fawood or Curzon Crescent using the **Subject Access Request (SAR) letter template and form** that can be found at the back of this document or can be downloaded as an electronic copy from our website at www.curzoncrescent.org.uk

You may request a Subject Access Request by any means you feel appropriate - including but not limited to verbally, by email or by our SAR template form. We ask, where possible, requestors use the Template and Form contained in the annex to this document. This is to ensure that we understand the nature of the request as quickly and clearly as possible; however, we will accept requests in any form.

The SAR Form must be submitted directly to the office or via the email admin@fawoodcc.brent.sch.uk (for Fawood requests), or admin@curzon.brent.sch.uk (for Curzon requests) to avoid delay in dealing with the request.

We aim to deal with SARs efficiently and transparently and will consult with the requester about how best we can provide the information requested. We will ask the requester about their preferred method of receiving the information. However, in cases where supplying a copy of the requested information in a hard copy would result in disproportionate effort, we would evaluate the particular circumstances of each request and reach agreement with the requester as to an alternative way of satisfying the request.

We will ascertain the most appropriate and secure way to provide you with the information.

Charges for SARs

A Subject Access Request is **free of charge**. However, we have the right to charge a reasonable administrative-cost fee should the request be excessive (i.e. involves complex data retrieval) or repetitive (i.e. involves additional copies of information already provided) which imposes a disproportionate administration burden on the school. We will provide evidence of how we make this decision about a request being excessive where appropriate.

Confirming the requester's identity

We will ask the requester for some form of ID to ensure that the person making the request is the individual to whom the personal data relates (or a person authorised to make a SAR on their behalf). We will also check that we have the requester's correct postal address.

When dealing with SARs for personal data relating to a pupil, we will clarify whether the requester has parental responsibility for the child or has the authorisation to act on their behalf.

Forms of Identification we will require:

Photo ID

- Passport
- Driving Licence
- Birth certificate

Proof of address

- Bank statement and/ or utility bill

Making a SAR on behalf of someone else

If the requester is making a SAR on behalf of someone else (the 'Data Subject'), we need to be satisfied that the 'third party' requester making the request is entitled to act on behalf of the Data Subject. It is the responsibility of the third-party requester to provide evidence of this entitlement.

We have discretion in deciding whether information in response to a SAR is disclosed to a third party who has made the SAR on behalf of the Data Subject or disclosed directly to the Data Subject. If disclosed directly to the Data Subject, then the Data Subject can choose to share the information with the third party if they wish.

Clarifying a SAR

Before we respond to a SAR, we may ask for additional information from the requester to enable us to find the personal data covered by the request.

Each SAR received will be acknowledged and once the necessary ID checks have been satisfied and clarification sought regarding the context of the personal data being requested, we will inform the requester of the date by which the response must be provided.

How long will information resulting from a SAR be available?

In accordance with the GDPR regulations, we will provide the required information within one month from the date

- we have satisfactorily confirmed the identity of the requester, and
- we have clarified/agreed the nature and requirements of the information being requested

We aim to respond to requests within the required time period of one month. Whilst we will strive to comply with the request within the timeframes above, requestors should keep in mind that during holiday periods or during exceptional occasions of school closure, staffing may be limited which may impact on how quickly we are able to respond to your request. In these circumstances, we will endeavour to keep you informed and deal with your request as quickly as possible. Where necessary we may have the right to extend this period for a further month (exceeding no more than 2 months).

If there is a delay in dealing with the request for any reason, we will contact the requester to explain the reason and to reach a mutually agreed alternative time period.

Information that is exempt from SARs

Certain types of personal data are exempt from SARs because of its nature or effect its disclosure may have (e.g. safeguarding or legal issues) or where disclosure would involve information about another individual. In these cases, we will explain to the requester the reasons why information requested cannot be disclosed.

How information is provided

Our responses to a SAR will include an explanation of the searches that have been made to deal with the request and the information revealed by those searches so that the requester is able to understand whether they have received all the information they are entitled to.

Monitoring our compliance with responding to SARs

We retain a log of SARs received which includes the details of requests received which we update to monitor progress as the SAR is processed. The log contains copies of the information supplied in response to the SAR together with copies of any material withheld and an explanation why.

We also monitor the time period for responding to SARs as well as deal with requests that have not been dealt with within the one-month timeframe.

Compliance with dealing and responding to SARs is monitored and discussed at senior leadership level and with our Governors.

Complaints about our Subject Access request procedure

If the requester believes that a request for information has not been dealt with properly, the requester should make a complaint through our normal complaints' procedure. If following the conclusion of the complaints procedure the requester is still dissatisfied or the original decision is not reviewed, the requester can complain directly to the Information Commissioner's Office on 0303 123 1113 or at www.ico.org.uk/concerns

The documents relating to a SAR are in the appendixes of this policy.

A. SAR Form

B. SAR for a child

C. SAR responding to a request

D. SAR responding to a request – Delay

Data Retention

Data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Data will only be retained for the specified period outlined in the records management schedule that the school has adopted and will be destroyed in a secure manner thereafter.

The Partnerships follows the IRMS Retention Schedule.