20 – GENERAL DATA PROTECTION REGULATION (GDPR) POLICY – v2

Let Us Play Scheme

(Play Scheme for children with profound
and multiple learning difficulties)
Registered Charity No 1072059

Name of Unit/Premises/School	**Let Us Play Scheme / St. Francis School**
Date of Policy Issued/Review	**06 April 2020**
Name of Chairperson	**Juliet Cheriton-Gerrard**
Signature of Chairperson	
Management Committee Name	**Matthew Lewis**
Management Committee Signature	

POLICY STATEMENT

This policy is in response to the new GDPR which came into effect on 25 May 2018. The GDPR replaces the Data Protection Act (1994) and whilst broadly similar in principle, requires a review and update on how LUPS handles and stores personal data.

RIGHTS UNDER GDPR

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

GENERAL POLICY

- LUPS will have a policy for how to record requests they will receive verbally.
- LUPS will understand when they can refuse a request and are aware of the information they will need to provide to individuals when they do so.
- LUPS will have processes in place to ensure that they will respond to a request for rectification without undue delay and within one month of receipt.
- LUPS will are aware of the circumstances when they can extend the time limit to respond to a request.

THE RIGHT TO BE INFORMED

LUPS will provide individuals, staff and parents/carers with all the following privacy information:

- The name and contact details of our organisation.
- The contact details of our data protection officer (DPO).
- The purposes of the processing.
- The lawful basis for the processing.
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations.
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).
- LUPS will provide individuals with privacy information at the time personal data is collected from them.
- If LUPS obtains personal data from a source other than the individual it relates to, LUPS will provide them with privacy information within a reasonable of period of obtaining the personal data and no later than one month.
- If LUPS plans to communicate with the individual, at the latest, when the first communication takes place; or
- If LUPS will plan to disclose the data to someone else, at the latest, when the data is disclosed.

LUPS will provide the information in a way that is:

- Concise;
- Transparent;
- Intelligible;
- Easily accessible; and
- Uses clear and plain language.

LUPS will regularly review and, where necessary, update our privacy information. If LUPS plans to use personal data for a new purpose, they will update their privacy information and communicate the changes to individuals before starting any new processing. LUPS will periodically undertake an information audit to find out what personal data is held and what they do with it.

THE RIGHT OF ACCESS

- LUPS will know how to recognise a subject access request and will understand when the right of access applies.
- LUPS will understand the nature of the supplementary information they will need to provide in response to a subject access request.
- LUPS will have processes in place to ensure that they will respond to a subject access request without undue delay and within one month of receipt.
- LUPS will are aware of the circumstances when they can extend the time limit to respond to a request.
- LUPS will understand that there is a particular emphasis on using clear and plain language if they are disclosing information to a child.
- LUPS will understand what they will need to consider if a request includes information about others.

THE RIGHT TO RECTIFICATION

- LUPS will know how to recognise a request for rectification and they will understand when this right applies.
- LUPS will have appropriate systems to rectify or complete information, or provide a supplementary statement.
- LUPS will have procedures in place to inform any recipients if they rectify any data they have shared with them.

THE RIGHT TO ERASURE

- LUPS will know how to recognise a request for erasure and they will understand when the right applies.
- LUPS will understand that there is a particular emphasis on the right to erasure if the request relates to data collected from children.

- LUPS will have procedures in place to inform any recipients if they erase any data they have shared with them.
- LUPS will have appropriate methods in place to erase information.

THE RIGHT TO RESTRICT PROCESSING

- LUPS will know how to recognise a request for restriction and they will understand when the right applies.
- LUPS will have appropriate methods in place to restrict the processing of personal data on our systems.
- LUPS will have appropriate methods in place to indicate on our systems that further processing has been restricted.
- LUPS will understand the circumstances when they can process personal data that has been restricted.
- LUPS will have procedures in place to inform any recipients if they restrict any data they have shared with them.
- LUPS will understand that they will need to tell individuals before they lift a restriction on processing.

THE RIGHT TO DATA PORTABILITY

- LUPS will know how to recognise a request for data portability and they will understand when the right applies.
- LUPS can transmit personal data in structured, commonly used and machine-readable formats.
- LUPS will use secure methods to transmit personal data.

THE RIGHT TO OBJECT

- LUPS will know how to recognise an objection and they will understand when the right applies.
- LUPS will have clear information in our privacy notice about individuals' right to object, which is presented separately from other information on their rights.
- LUPS will understand when they will need to inform individuals of their right to object in addition to including it in our privacy notice.
- LUPS will have appropriate methods in place to erase, suppress or otherwise cease processing personal data.

RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND PROFILING

LUPS is, and will, not be required to conduct automated decision making and profiling. Should the requirement for this process come forward, this policy will be required to be updated and approved by the Committee and updated privacy guidelines given to all parties affected prior to the operation taking place.

ACCOUNTABILITY AND GOVERNANCE

- LUPS will take responsibility for complying with the GDPR, at the highest management level and throughout our organisation.
- LUPS will keep evidence of the steps LUPS will take to comply with the GDPR.
- LUPS will put in place appropriate technical and organisational measures, such as:
    - adopting and implementing data protection policies (where proportionate);
    - taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations;
    - putting written contracts in place with organisations that process personal data on our behalf;
    - maintaining documentation of our processing activities;
    - implementing appropriate security measures;
    - recording and, where necessary, reporting personal data breaches;
    - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests;
    - appointing a data protection officer (where necessary); and,
    - adhering to relevant codes of conduct and signing up to certification schemes (where possible).

DOCUMENTATION

- LUPS will document all the applicable information under Article 30(1) of the GDPR.
- LUPS will document all the applicable information under Article 30(2) of the GDPR.
- LUPS will document our processing activities in writing.
- LUPS will conduct regular reviews of the personal data they process and update our documentation accordingly.

When preparing to document processing activities LUPS will:

- do information audits to find out what personal data our organisation holds;
- distribute questionnaires and talk to staff across the organisation to get a more complete picture of our processing activities; and,
- review our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.

As part of our record of processing activities LUPS will document, or link to documentation, on:

- information required for privacy notices;
- records of consent;
- controller-processor contracts;
- the location of personal data;
- Data Protection Impact Assessment reports; and
- records of personal data breaches.

LUPS will document processing activities in electronic form so they can add, remove and amend information easily.

SECURITY

- LUPS will undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security they will need to put in place.
- When deciding what measures to implement, LUPS will take account of the state of the art and costs of implementation.
- LUPS will have an information security policy (or equivalent) and take steps to make sure the policy is implemented.
- Where necessary, LUPS will have additional policies and ensure that controls are in place to enforce them.
- LUPS will make sure that they regularly review our information security policies and measures and, where necessary, improve them.
- LUPS understands that they may also need to put other technical measures in place depending on our circumstances and the type of personal data LUPS will process.
- LUPS will use encryption and/or pseudonymize where it is appropriate to do so.
- LUPS will understand the requirements of confidentiality, integrity and availability for the personal data they process.
- LUPS will make sure that they can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.
- LUPS will ensure that any data processor they use also implements appropriate technical and organisational measures.
- LUPS will know how to recognise a personal data breach.
- LUPS will understand that a personal data breach isn't only about loss or theft of personal data.
- LUPS will have prepared a response plan for addressing any personal data breaches that occur.
- LUPS will have allocated responsibility for managing breaches to a dedicated person or team.
- Our staff will know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.
- LUPS will know who the relevant supervisory authority for our processing activities is.
- LUPS will have a process to notify the Information Commissioner's Office (ICO) of a breach within 72 hours of becoming aware of it, even if LUPS does not have all the details yet.
- LUPS will know what information they must give the ICO about a breach.
- LUPS will have a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
- LUPS will know they must inform affected individuals without undue delay.

- LUPS will know what information about a breach they must provide to individuals, and that they should provide advice to help them protect themselves from its effects.
- LUPS will document all breaches, even if they don't all need to be reported.

SUMMARY

Data protection is primarily based around common sense and decency. The data obtained by LUPS will be used solely for the purpose of running the play scheme and no other purposes. All data processes will be conducted by staff or committee who are trusted and aware of the criteria to be met in this policy.

ASSOCIATED POLICY'S

- Safeguarding Children Policy
- Complaints Policy
- Booking Policy
- Equality & Diversity Policy
- Admissions Policy
- Disciplinary Procedures Policy
- Left Behind Child Policy
- Administration of Medication