

Data Protection Policy

Data Protection Policy Version Control	
Date of Approval	June 2022
For Review	June 2024
Document Owner	Governance Lead
Current Version	1.0

1. Definitions

Organisation	The Museum of Childhood Ireland, a charity registered under number 20205452
DPA	The Irish Data Protection Act 2018 which implements the EU’s General Data Protection Regulation.
Responsible Person	The individual responsible for Data Protection matters for the Museum in this case Cian Spillane

2. Context & Scope

It is important to note that the Museum of Childhood Ireland processes a very limited amount of personal data. This policy affirms the commitment of the Museum in ensuring that all personal data processed by the organisation is processed in line with best practice and legislative requirements.

3. Data protection principles

The Organisation is committed to processing data in accordance with its responsibilities under the DPA.

DPA requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the DPA in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

4. General provisions

- This policy applies to all personal data processed by the Organisation.
- The Responsible Person shall take responsibility for the Organisation's ongoing compliance with this policy.
- This policy shall be reviewed at least every three years.

5. Lawful, fair and transparent processing

- Individuals have the right to access their personal data and any such requests made to the Organisation shall be dealt with in a timely manner.

6. Lawful purposes

- All data processed by the Organisation must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
- Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
- Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Organisation's systems.

7. Data minimisation

- The Organisation shall ensure that personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

8. Accuracy

- The Organisation shall take reasonable steps to ensure personal data is accurate.

- Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

9. Archiving / removal

- To ensure that personal data is kept for no longer than necessary, the Organisation shall periodically review its records and update accordingly.

10. Security

- The Organisation shall ensure that personal data is stored securely
- Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.
- When personal data is deleted this should be done safely such that the data is irrecoverable.

11. Breach

- In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Organisation shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the Data Protection Commission.