CYM

THE INSTITUTE FOR CHILDREN, YOUTH & MISSION

DATA PROTECTION (GDPR) POLICY

cym.ac.uk

hello@cym.ac.uk
0115 7770102

Charity No. 1081144

Policy name	Data Protection (GDPR) Policy
Purpose of policy	To set out the Institute's approach to Data Protection
Approval given by	Board of Trustees
Last review date	July 2023
Review due date	July 2024
Responsible for review	Sarah Fegredo, Chair of Trustees

1. Background

1.1 Personal data is information which relates to a living individual and from which they can be identified, either directly or indirectly.

1.2 Personal data is held at the Institute in a variety of ways and for many different purposes. These purposes include, but are not limited to, the maintenance of staff and student records and other matters such as research data and the relationships with alumni, supporters, marketing contacts and other persons.

1.3 Personal data will be handled with care and in compliance with the law governing data protection, the General Data Protection Regulation (GDPR)

1.4 This policy sets out the commitment of the Institute to the maintenance of high standards of protection for the personal data it holds, whether in digital or manual records.

2. Scope

2.1 The Institute confirms its commitment to compliance with the GDPR.

2.2 This policy covers all Institute activity in which personal data is used. It applies to all members of the Institute including staff, students, trustees and others acting for or on behalf of the Institute or who are otherwise given access to the Institute's information infrastructure.

2.3 This policy should be read and interpreted in conjunction with the other related Institute policies and partner University procedures which are relevant to this policy.

3. Registration at the Information Commissioner's Office

3.1 The Institute maintains and complies with its registration at the Information Commissioner's Office in accordance with the requirements of the GDPR and is committed to co-operating with the Office in the fulfilment of its obligations and support of the principles underpinning data protection law.

4. Principles governing the processing of personal data

In compliance with Article 5 of the GDPR, personal data will be:
4.1 processed lawfully, fairly and in a transparent manner

4.2 collected for specific, explicit and legitimate purposes

4.3 adequate, relevant and limited to what is necessary for the purpose

4.4 accurate and kept up to date

4.5 only kept for as long as it is needed

4.6 kept safe using appropriate technical and organisational measures

5. The legal basis for processing

5.1 The Institute makes Privacy Statements readily available to students, staff and others. Privacy Statements set out the type of data generally held by the Institute, the reasons for the collection of the personal data, an explanation about circumstances in which data may be shared with others and a statement of the rights of individuals under the GDPR.

5.2 Individuals will be informed of the lawful basis for the intended processing of their personal data. In the case of students and staff the lawful basis will generally be the need to fulfil the contract between the individual and the Institute.

5.3 If there is an intention to use the data for marketing purposes or other purposes where the Institute is relying on consent as the lawful basis for processing, the individual will be notified of this intention and will be asked for clear and specific consent before any such use will be made of the data. The Institute will maintain records of consents given and withdrawn.

6. Use and disposal of Data

The Institute has processes in place to ensure that the personal data it holds remains accurate and up to date and is disposed of in accordance with its Data Classification and Handling Policy. In particular:

6.1 The Institute will seek to maintain high standards of data integrity and aim to avoid duplication, inaccuracy and inconsistencies across personal data retention locations.

6.2 The Institute will maintain a comprehensive Retention of Records Policy to help avoid excessive retention or premature destruction of personal data.

6.3 Personal data which is no longer required, or which should no longer be held under GDPR will be disposed of in a manner appropriate to its nature and the need for security in accordance with its Data Classification, Handling and Disposal Policy.

6.4 The Institute will maintain an Information Asset Register detailing all processing activity including the data held, its source, details of sharing of the data and the lawful basis for the processing.

7. Security

The Institute will maintain appropriate technical and organisational measures to ensure the security of personal data. In particular:

7.1 Data security is created, reviewed, tested and improved on an on-going basis

7.2 Procedures are in place to analyse and respond to any identified threats to data security

7.3 Policies specifically relating to digital security measures are listed at the end of this policy

8. Risk Management

8.1 The Institute assesses and identifies areas that could cause data protection compliance or security problems and records these through the Institute's risk registers which is actively managed. Controls are applied to mitigate the identified risks and these are regularly verified for effectiveness as part of this process.

8.2 The Institute acknowledges its duty under GDPR to conduct a Data Protection Impact Assessment when introducing new technologies or procedures which may involve a high risk to the rights and freedoms of individuals.

9. The rights of data subjects

The rights of data subjects under GDPR will be respected. In particular:

9.1 the Institute recognises that data subjects have the right to have access to the personal data held about them; to have errors corrected; to have data erased in some circumstances; to object to or to restrict processing in some circumstances; to have data securely transferred to another organisation; and to assert the right to human intervention, to express their opinion and to obtain and challenge explanations where automated decision-making is used and has an impact on them;

9.2 the Institute will respond to requests for access to data or the assertion of other GDPR rights within the statutory time limits in accordance with its Access Request Procedure.

10. Sharing data with other organisations

10.1 Data may be shared with other organisations in accordance with the Institute Privacy Statements and as permitted by law.

10.2 The Institute enters into written agreements with all processors of personal data controlled by the Institute which comply with the stipulations of GDPR

10.3 Data is only transferred outside the EEA in compliance with the conditions for transfer set out in GDPR. In particular, personal data will only be transferred to territories outside the EEA where there are adequate standards of privacy protection, by virtue of national laws or via contractual arrangements, and in other circumstances where transfers are permitted by GDPR. The Institute takes steps to ensure that there are adequate safeguards and data security in place and has measures to audit security arrangements on a periodic basis.

10.4 Mechanisms are in place to notify third parties, where required, of any change in the status of consent given by a data subject where consent is the lawful basis for the processing of data.

11. Staff training and personal responsibility

11.1 The Institute provides data protection training for all staff. This is done as part of the on-boarding procedure for new staff and when updates are required. Completion of data protection training is an essential element of a successful probation. The training reinforces personal responsibility and good security behaviours, including how to recognise and report breaches and the safe movement of data through appropriate channels.

11.2 Specialist training is provided to staff with specific roles, such as marketing, information security, and Human Resources.

11.3 Breaches of this or a related policy will be dealt with in accordance with the Institute's Disciplinary Procedure.

12. Roles and Responsibilities

12.1 The Institute has a designated Data Protection Officer, the Director of Operations, with overall responsibility for data protection compliance in accordance with the duties set out in GDPR.

12.2 The Data Protection Officer is responsible for:

12.2.1 Maintaining this policy and all records relating to data protection;

12.2.2 Providing guidance, support, training and advice on compliance with GDPR;

12.2.3 Liaison with the Information Commissioner's Office;

12.2.4 Taking legal advice on matters relating to the GDPR where necessary;

12.2.5 Supervising the management of access and other requests from data subjects;

12.2.6 Managing the procedure for the reporting and resolving of personal data breaches;

12.2.7 Reviewing and auditing the way personal information is managed, and ensuring that methods of handling personal information are regularly assessed and evaluated;

12.2.8 Monitoring and reporting on compliance with data protection training.

12.3 The Director of Operations is responsible for ensuring awareness of and compliance with this policy in their areas

12.4 Principal investigators are responsible for personal data management in their own research studies and for ensuring that secure information systems and operating procedures are in place with regards to data handling. Where personal data is processed, research staff and students must adhere to the personal data processing requirements set out in this policy, as well as the Institute's Code of Practice for Research.

12.5 Staff training reinforces personal responsibility and good security behaviours, including how to recognise and report breaches

13. Identifying and resolving personal data breaches

The Institute has a procedure for the reporting of breaches to the appropriate individuals as soon as they are discovered, and to investigate and implement recovery plans. This procedure is part of the Institute's Incident Management process and includes assessment of the likely risk to individuals and, if required, notification of affected individuals and reporting to the Information Commissioner's Office in line with GDPR requirements.

14. Reporting and Governance

The Institute has a process to monitor compliance with this policy and related policies. The Institute Senior Leadership Team receives an annual report from the Data Protection Officer, as does the Audit and Risk Committee of the Board of Trustees. Data protection at the Institute is monitored as part of the annual internal audit plan.

END