ICOT College Data Protection Policy v1.0

1. Purpose and Commitment

The International College of Technology (ICOT) is committed to protecting the rights and freedoms of data subjects and to processing personal data securely and lawfully, in compliance with the Data Protection Acts 1988–2018 and the General Data Protection Regulation (GDPR).

This policy outlines ICOT's obligations and staff responsibilities in managing personal data.

2. Scope

This policy applies to all personal data processed by ICOT, including data relating to students, staff, contractors, and any other individuals, regardless of format (electronic or paper).

3. Data Protection Principles

ICOT shall comply with the seven principles of GDPR. Personal data must be:

1. Processed lawfully, fairly, and in a transparent manner.
2. Collected for specified, explicit, and legitimate purposes (Purpose Limitation).
3. Adequate, relevant, and limited to what is necessary (Data Minimi**s**ation).
4. Accurate and, where necessary, kept up to date (Accuracy).
5. Kept in a form which permits identification of data subjects for no longer than is necessary (Storage Limitation).
6. Processed in a manner that ensures appropriate security (Integrity and Confidentiality).
7. ICOT is responsible for, and must be able to demonstrate, compliance with these principles (Accountability).

4. Governance and Accountability

4.1. Data Protection Officer (DPO)

- The appointed DPO for ICOT is: Shiam Rahman, dpo@icot.ie
- The DPO is responsible for monitoring compliance with GDPR, managing data subject requests, advising on Data Protection Impact Assessments (DPIAs), and acting as the point of contact for the Data Protection Commission (DPC).
- **DPO Training:** The DPO's CV, detailing relevant and ongoing data protection training, is held on file at **Google Drive**.

4.2. Record of Processing Activities (ROPA)

- ICOT maintains a detailed ROPA (as provided to QQI) which documents all data processing activities, including data categories, purposes, lawful bases, and retention periods.

4.3. Data Protection Impact Assessments (DPIAs)

- ICOT will conduct a DPIA for any new processing activity that is likely to result in a high risk to the rights and freedoms of individuals (e.g., new surveillance technology, new large-scale student management system).
- **Evidence:** A log of all DPIAs conducted is maintained by the DPO at: *Google `Cloud\IT\DPO_GDPR\Compliance\4_Logs\ICOT_DPIA_Log`*.

4.4. Staff Training

- All staff who handle personal data will receive mandatory data protection training upon induction and annually thereafter.
- **Evidence:** Training completion records are maintained at: *Google `Cloud\IT\DPO_GDPR\CPD`*

5. Lawfulness of Processing and Consent

5.1. Lawful Basis

- ICOT will only process personal data if a valid lawful basis exists, such as:
    - The data subject has given **consent**.
    - Processing is necessary for the performance of a **contract** (e.g., student enrolment).
    - Processing is necessary for compliance with a **legal obligation**.
    - Processing is necessary for ICOT's **legitimate interests** (and does not override the individual's rights).

5.2. Consent Mechanisms

- Where processing is based on consent, it must be freely given, specific, informed, and unambiguous, obtained via a clear affirmative action.
- Requests for consent will be separate from other terms and conditions.
- **Evidence:** Records of consent (e.g., signed enrolment forms, timestamped digital checkboxes) are maintained in: Academic Management System -> Student files.

5.3. Website and Cookies

The ICOT website must have a clear cookie policy and a compliant cookie consent banner.

- **Action: No non-essential trackers** (e.g., marketing, analytics, third-party trackers sending data to the US) shall be activated *before* a user gives explicit "opt-in" consent.
- The DPO and IT/Web team must conduct an immediate audit of the website to remove or modify any non-compliant trackers.

5.4. Data Minimisation

- ICOT will only collect, process, and store the personal data that is absolutely necessary for the stated purpose. Personal data will not be collected on a "just in case" basis.

6. Data Subject Rights

Data subjects have the right to:

- **Access:** Request a copy of their personal data.
- **Rectification:** Request correction of inaccurate data.
- **Erasure ("Right to be Forgotten"):** Request their data be deleted, under certain conditions.
- **Restriction:** Request that processing of their data be restricted.
- **Portability:** Request that their data be transferred to another controller.
- **Objection:** Object to processing (e.g., for direct marketing).

6.1. How to Exercise Rights

- Data subjects (students, staff) may exercise their rights by submitting a written request to the DPO at: dpo@icot.ie
- ICOT will respond to all Subject Access Requests (SARs) within one calendar month.

7. Security of Personal Data

ICOT will implement appropriate security measures to protect personal data.

7.1. Technical Measures

- Technical security measures (including firewalls, encryption, access control, antivirus, etc.) are detailed in the **ICOT IT Security Policy**.

7.2. Physical Measures

- Physical security measures include: [e.g., Locked offices, secure filing cabinets for paper records, a clean desk policy, building access control, alarm system]

7.3. Administrative Measures

- Administrative security measures include: [e.g., Confidentiality clauses in staff contracts, this policy, staff training, Role-Based Access Controls (RBAC)]

8. Third Parties and International Transfers

8.1. Data Processing Agreements (DPAs)

- ICOT will **not** share personal data with any third-party processor (e.g., accountants, cloud software providers, HR services) until a GDPR-compliant Data Processing Agreement (DPA) is in place.
- **Action:** The DPO is to conduct an audit of all third-party vendors to ensure DPAs are in place.
- **Evidence:** A register of all third-party vendors and their associated DPAs is maintained at: *Google Cloud\IT\DPO_GDPR\Compliance\5_Vendor Register*.

8.2. International Transfers

- ICOT will not transfer personal data outside the European Economic Area (EEA) unless:
    1. The country has an adequacy decision from the European Commission (e.g., the UK).
    2. Appropriate safeguards, such as Standard Contractual Clauses (SCCs), are in place.
- **Action:** This applies to service providers (e.g., US-based website trackers) and any transfers to the UK. All such vendors must have SCCs or other safeguards in place.

9. Personal Data Breach Management

9.1. Identification and Response

- Any staff member or student who suspects a personal data breach (e.g., email sent to the wrong recipient, lost laptop, unauthori**s**ed access) must report it **immediately** to the DPO at dpo@icot.ie and the IT Helpdesk.
- The DPO will activate the Incident Response Plan to contain and assess the breach.

9.2. Notification

- If the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO will notify the Data Protection Commission (DPC) within 72 hours of becoming aware of it.
- If the risk is high, the affected individuals will also be notified.

9.3. Data Breach Incident Log

- **Evidence:** All data breaches, including minor incidents and "near-misses," will be recorded in a Data Breach Incident Log maintained by the DPO.
- This log is located at: `Cloud\IT\DPO_GDPR\Compliance\4_Logs\ICOT_Security_Incident_Log.gsheet`

10. Policy Review

This policy will be reviewed annually, or following significant changes to legislation or ICOT's processing activities, by the DPO.

- **Next Scheduled Review:** *November 2026*