INTERNATIONAL COLLEGE

ROBERT GORDON UNIVERSITY ABERDEEN

International College Robert Gordon University (ICRGU)
CPR M2: Data Protection Policy
Version 2020/01

1. Purpose

1.1. This data protection policy ensures the Company:

i. Complies with the EU General Data Protection Regulation (GDPR) as well as relevant local legislation, and follows good practice
ii. Protects the data privacy and protection rights of staff, students, business partners and all other stakeholders
iii. Is open about how it processes individuals' data
iv. Protects itself from the risks of a data breach
v. Facilitates the rights of individuals under the GDPR
vi. Ensures ongoing adherence and improvements to data privacy and protection practices.

2. Data Protection Principles

2.1. The Company is committed to processing data in accordance with its responsibilities under the GDPR. Article 5 of the GDPR requires that personal data shall be:

i. processed lawfully, fairly and in a transparent manner in relation to individuals;
ii. 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;
iii. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
iv. 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;
v. 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 GDPR in order to safeguard the rights and freedoms of individuals; and
vi. 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.

3. General Provisions

3.1. This policy applies to all personal data processed by the Company under the GDPR.
3.2. Reporting into the Navitas Leadership Team, the Europe Data Protection Officer shall take responsibility for the Company's ongoing compliance with this policy.
3.3. The Company shall register with the Information Commissioner's Office as an organisation that processes personal data.

4. Data Transparency and Openness

4.1. At the point of their personal data collection all individuals shall be guided to the Company's privacy notice for a simple, clear explanation of how their data will be processed, with whom it may be shared and how they can make further queries in regard of that data.

4.2. Individuals have the right to access their personal data and any such requests made to the Company shall be dealt with in a timely manner.
4.3. The Company shall maintain procedures to allow the same. To ensure its processing of data is lawful, fair and transparent, the Company shall maintain an appropriate set of policies, procedures, data protection handbooks and training materials.
4.4. These shall be reviewed at least annually.

5. Lawful Purposes

5.1. All data processed by the Company must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests
5.2. The Company shall record the appropriate lawful basis in the Lawful Basis for Processing Personal Data document.
5.3. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be maintained
5.4. Where Legitimate Interest is relied upon then the rationale shall be documented within the Lawful Bases for Processing Personal Data document.
5.5. 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 Company's systems.

6. Data Minimization

6.1. The Company shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
6.2. Article 9 data shall only be collected with permission of the DPO or the Data Protection Managers. Article 9 data consists of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

7. Data Accuracy

7.1. The Company shall take reasonable steps to ensure personal data is accurate.
7.2. 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.

8. Storage Limitation

8.1. The Company shall maintain a Record Management, Retention and Disposal policy to guide staff on how to handle records and documents and to understand record retention and disposal requirements
8.2. To ensure that personal data is kept for no longer than necessary, the Company shall establish and maintain a Data Retention Schedule for each category of data processed.
8.3. The Data Retention Schedule shall consider what data should/must be retained, for how long, and also take into account national law requirements outside of the GDPR.

9. Data Confidentiality

9.1. The Company shall maintain an Information Security policy that outlines how the Company provides Information Security and to reassure all parties involved with the Company that their information is protected and secured. In particular it shall address the following;
9.2. The Company shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
9.3. Access to personal data shall be limited to people who need access and appropriate security shall be in place to avoid unauthorised sharing of information. This is referred to as role-based access.
9.4. When personal data is deleted this should be done securely such that the data is irrecoverable.
9.5. Appropriate back-up and disaster recovery solutions shall be in place, tested and a record of such maintained.

9.6. Where personal data is shared within the business or with external organisations then its privacy and protection shall be governed by appropriate documentation and safeguards.

10. Data Breach

10.1. 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 Company shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the ICO.
10.2. The Company shall maintain a Data Breach procedure that ensures notification can be made to the ICO within the required 72 hours
10.3. The Company shall also maintain a simple Data Breach guide for rapid reference.

11. Individual Rights

11.1. The Company shall main suitable DSAR procedures to facilitate the individual's data privacy and protection rights as defined in Articles 15-21 namely;

- Right of Access by the data subject
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object

12. Compliance

12.1. The Company shall maintain a Data Protection organisational structure that allows the effective discharge of its data privacy and protection obligations
12.2. The Company shall maintain a Privacy by Design policy and ensure its implementation into all business and project activities that involve the processing of personal data
12.3. The Company shall ensure that all staff have access to simple, clear guidance in the form of a Data Protection Handbook to allow them to deliver their duties in a GDPR compliant manner
12.4. All staff shall undergo GDPR Training to awareness level at least and such records maintained.
12.5. The Company shall maintain an Audit schedule such that all sites and shared services functions are audited at least annually using an appropriate site audit checklist.
12.6. An annual organisational GDPR audit shall also be performed for which an Internal Audit checklist shall be maintained
12.7. The Company shall conduct appropriate and regular Information Security testing and remediate accordingly
12.8. All staff shall undergo refresher training on data privacy and protection every two years at least.

13. Continuous Improvement

13.1. The Company shall seek feedback from individuals on a continuous basis as to how current practice could be improved
13.2. Audits shall be conducted to be educational and supportive and allow the sharing of best practice across the organisation
13.3. The Company shall subscribe and participate in appropriate organisations, forums, news sources etc to allow global development and best practices to be monitored and effectively disseminated within the business.