City & Guilds Group
Group Privacy Policy

1 Scope and Application

1.1 This policy applies to The City and Guilds of London Institute, its subsidiaries, business units and brands (together the "**City & Guilds Group**"). The City & Guilds Group is committed to establishing and maintaining a culture of privacy compliance.

1.2 This policy describes the City & Guilds Group's approach to the protection of the personal data of individuals, and the exercise of data protection rights by individuals, whose personal data are processed by one or more members of the City & Guilds Group in accordance with applicable data protection laws, including General Data Protection Regulation (EU) 2016/679 (**GDPR**).

1.3 This policy establishes a framework for a consistent approach to privacy by design throughout the City & Guilds Group in order to ensure proper stewardship and use of personal data.

1.4 This policy applies to all business activities that may involve the processing of personal data undertaken by a member of the City & Guilds Group or by any person working under the direction or control of a member of the City & Guilds Group. This includes members of the Management Board, Trustee Board, officers, employees, and any third party entity or person granted access to personal data in the custody or control of a member of the City & Guilds Group.

2. Definitions

Data Subject: any individual about whom a member of the City & Guilds Group processes Personal Data. Members of the City & Guilds Group process information from (or pertaining to) various groups of individuals including customer contacts, supplier contacts, employees, apprentices, and learners who have contact with one or more members of the City & Guilds Group through its third party relationships such as with customers, suppliers, independent contractors, consultants, and other business partners.

Controller: a natural or legal person, public authority, agency or any other entity or person who alone or jointly with others determines the purposes and means of processing the personal data.

Information Security Event: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Personal Data: any information relating to an identified or identifiable natural person (ie a data subject). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Processor: a natural or legal person, public authority, agency or any other entity or person who alone or jointly with others processes Personal Data on behalf of the Controller.

Process, processed or processing: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated

means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Special Categories of Personal Data: Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning health or data concerning a natural person's sex life or sexual orientation.

4 Data Protection Principles

The core principles relating to the processing of Personal Data are described in this section.

- Lawfulness, Fairness and Transparency Principle
- Purpose Limitation Principle
- Data Minimisation Principle
- Accuracy Principle
- Storage Limitation Principle
- Integrity and Confidentiality Principle
- Accountability Principle

4.1 **Lawful, fair and transparent**: this principle requires that processing of Personal Data be lawful under one more of the following legal justifications:

- with valid consent from the Data Subject;
- where necessary for the legitimate interests of a member of the City & Guilds Group or a third party;
- where necessary to perform a contract with the Data Subject;
- where necessary for compliance with a legal obligation to which the Controller is subject;
- where necessary to protect the vital interests of the Data Subject or another natural person; and
- where necessary to perform a specific task carried out in the public interest.

Processing Special Categories of Personal Data: Special Categories of Personal Data will not be processed unless one or more of the specific legal justifications set out in the GDPR are met, which shall be determined by Group Legal in consultation with the Privacy Officer for the City & Guilds Group.

Transparency: use of Personal Data must be consistent with the purposes stated in the applicable privacy notice, and the Data Subject must be given the minimum information regarding such use as required by the GDPR.

4.2 **Purpose**: Personal Data collected by a member of the City & Guilds Group may only be processed in ways that are compatible with the purposes as stated in the applicable privacy notice provided, together with the following stated uses:

- **Quality control purposes and/or administration regarding learning, assessment, or certification**: members of the City & Guilds Group may process Personal Data relating to customer and supplier contacts, learners, employees, and apprentices which has been provided to it by organisations such as Employers, Centres, and Training Providers in order to undertake administration in relation to the qualification for which the Data Subject is registered, and to undertake quality assurance process, regulatory obligations, investigations, complaints, and appeals.

- **Administration of employment relationships**: members of the City & Guilds Group may collect and process Personal Data relating to personnel required to administer the employment relationship between the relevant member of the City & Guilds Group and the Data Subject.

Processing for new purposes: in order to use Personal Data for a new purpose not originally disclosed to the Data Subject at the time of collection, the relevant member of the City & Guilds Group must consider whether the new processing is compatible with the purposes for which the Personal Data was originally collected. Such considerations include:

- any links between the original purpose and the new purpose;
- the context in which the Personal Data have been collected;
- the nature of the Personal Data;
- possible legal or employment consequences to the Data Subject if the new processing occurs; and
- the existence of appropriate safeguards.

To the extent that the new purpose is incompatible with the original collection, the relevant member of the City & Guilds Group shall not be permitted to continue with the new purpose and should consult Group Legal and the Privacy Officer for the City & Guilds Group.

4.3 **Accuracy**: this principle requires that Personal Data within the City & Guilds Group's custody and control be accurate and kept up to date. Data Subjects may contact the City & Guilds Group to request that their Personal Data is updated, corrected, or completed.

4.4 **Data minimisation**: members of the City & Guilds Group will only Process the minimum types of Personal Data that are relevant, limited and necessary to achieve specific business objectives. Where possible, Personal Data will be aggregated, pseudonymised, or anonymised.

4.5 **Storage or retention limitation**: members of the City & Guilds Group shall keep Personal Data in a form which permits identification of a Data Subject for no longer than is necessary for the purposes for which the Personal Data was originally gathered and processed as stated in the applicable privacy notice. Information about a Data Subject will be deleted when it is no longer required to satisfy the stated purpose and accordance with the City & Guilds Group Data Retention Policy.

4.6 **Integrity and confidentiality**: in order to comply with the requirements of this principle, members of the City & Guilds Group must only process Personal Data in a manner that ensures appropriate security of the Personal Data, using appropriate technical and organisational measures, in accordance with the City & Guilds Group IT Security Policy. To safeguard against unauthorised access, all documents containing Personal Data, whether hard copy or in electronic form, must be safeguarded. Members of the City & Guilds Group must limit access to internal computing systems that hold Personal Data to authorised users who are given access to such systems through the use of a unique identifier and password and which are managed by assigned security administrators in Group IT.

4.7 **Accountability**: members of the City & Guilds Group must be able to demonstrate compliance with the foregoing principles through detailed documentation of processing operations. Members of the City & Guilds Group shall maintain an inventory of its processing operations with respect to Personal Data in the form of data maps, data

registers, and other documentation. Such documentation will include, amongst other information:

- **What is processed**: the name and contact details of the data controller; the purposes of processing; a description of the categories of data subjects, categories of personal data, and categories of recipients of the personal data; where applicable, transfer of personal data to a third country or international organisation; where possible, time limits for erasure of the different categories of personal data; and a general description of the technical and organisational security measures in place;

- **Where it is processed**: the inventory may also provide information as to where the Personal Data is held (i.e. servers, mobile devices, desktops, cloud environment, and geographic location) and where the personal data flows (i.e. within systems and processes, among vendors, and geographic regions).

5 Rights of Data Subjects

Members of the City & Guilds Group will provide measures by which the Data Subject has rights regarding access, rectification, correction, objection and portability. These rights are described in this section.

5.1 **Transparency / access**: any Data Subject may enquire as to the nature of the Personal Data stored or processed about him or her by any member of the City & Guilds Group, regardless of the location of the data processing and storage. The member of the City & Guild Group processing such Personal Data will respond to such request in accordance with the City & Guilds Group Data Subject Rights Policy.

5.2 **Rectification**: if any Personal Data is inaccurate or incomplete, the Data Subject may request that his or her Personal Data be amended or corrected. Data Subjects may contact the City & Guilds Group to request that their Personal Data is updated, corrected, or completed.

5.3 **Erasure**: in the event a Data Subject requests that his or her personal data be deleted, the custodian within the City & Guilds Group must contact the City & Guilds Group Privacy Officer who will determine whether a legitimate business reason continues to exist for retention of the Personal Data in accordance with the City & Guilds Group Data Subject Rights Policy. If there is no ongoing legitimate business reason, arrangements will be made of the erasure of the Personal Data.

5.4 **Restriction of, or objection to, processing**: the City & Guilds Group recognises that a Data Subject has the right to restrict and object to processing of his or her Personal Data. To the extent that a Data Subject notifies a member of the City & Guilds Group of its objection to the processing of his/her Personal Data, the City & Guilds Group shall suspend such processing until such time as the City & Guilds Group can demonstrate compelling legitimate grounds for such processing. The City & Guilds Group may cancel the suspension and resume its data processing activities once it has determined such legitimate grounds. Such grounds will include, without limitation, record retention, regulatory obligations, processing for the establishment, exercise or defence of legal claims.

5.5 **Data portability**: in response to a Data Subject's written request, in certain circumstances, the Data Subject is entitled to have his or her Personal Data transmitted to a Controller as identified by the Data Subject where technically feasible. On receipt of a request, the relevant member of the City & Guilds Group will review the request, and where appropriate,

promptly transfer the requested Personal Data in a structured, commonly used and machine readable format. The City & Guilds Group may retain a copy of the Data Subject's written request for record keeping purposes.

Each privacy notice will include detailed information about how a Data Subject may exercise his or her rights, including an email address and physical address.

Members of the City & Guilds Group will adhere to the City & Guilds Group Data Subject Rights Policy in addressing requests from Data Subjects to exercise their rights under the GDPR.

6 Data Protection by Design and Default

6.1 **By Design**: data protection "by design" requires taking data protection risks into account throughout the life cycle design of a new process, product or service. Members of the City & Guilds Group will implement technical and organisational measures to ensure that processing of Personal Data complies with applicable law and the rights of the Data Subject.

6.2 **By Default**: data protection "by default" requires mechanisms to be in place to ensure that only Personal Data which are necessary for each specific purpose are processed. Members of the City & Guilds Group will ensure such mechanisms are in place to implement the data protection principles described in section 4 above.

7 Inter-Group Transfer of Personal Data

A transfer of Personal Data from one legal entity to another is considered a data transfer between the two different entities. All transfers between different legal entities within the City & Guilds Group shall be carried out shall be carried out in accordance with country and regional regulatory requirements.

8 Information Security Event Notification

Upon discovery or learning of a potential or actual data breach or Information Security Event, employees of the City & Guilds Group are obligated to immediately report such event to the City & Guilds Group Privacy Officer. Data breaches and Information Security Events shall be dealt with in accordance with the Data Breach Policy of the City & Guilds Group.

9 Modifications to the Policy

9.1 The City & Guilds Group reserves the right to modify this policy as necessary to comply with changes in laws, regulations, practices and procedures, or requirements imposed by data protection authorities.

9.2 The City & Guilds Group will notify its employees and other Data Subjects of any changes to this Policy by posting the updated policy on relevant internal and external websites.