City & Guilds Group
Data Breach 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**).

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 a member of the City & Guilds Group, in accordance with applicable data protection laws, including Regulation (EU) 2016/679 (**GDPR**).

1.3. 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 (**personnel**).

1.4. This policy is in internal policy, and is available on the City & Guilds Group intranet, and to personnel. This policy may be made available, in PDF format, to external third parties on request.

2. Roles and Responsibilities

2.1. The Management Board has overall responsibility for ensuring adherence to this policy by all members of the City & Guilds Group.

2.2. Data Owners (as defined on the Group Data Protection SharePoint Site) are responsible for communicating this Policy within their responsible business area.

2.3. The City & Guilds Group Data Protection Team is responsible for:

- responding to queries about this policy - which may be sent to gdpr@cityandguilds.com;
- collecting feedback from Data Owners about this policy;
- reviewing this policy, as necessary, to ensure that it meets the requirements of applicable data protection laws.

3. Personal Data Breach Definition

3.1. A personal data breach is defined in Article 4.12 of the GDPR as:

> *"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."*

A personal data breach is considered to be any unintended or unexpected act or omission that affects or may affect the security, availability and/or integrity of personal data.

If appropriate measures are not taken in time, personal data breaches may result in breach of applicable data protection laws, as well as tangible or intangible damages to individuals - such as loss of control over their personal data, discrimination, identity theft, financial loss, reputational damage, loss of confidentiality, or other types social or economic loss.

3.2. This policy sets out the action protocol in the event that a personal data breach occurs regarding personal data processed by a member of the City & Guilds Group.

4. Notification of Breach

Where a member of staff of the City & Guilds Group becomes aware of any breach, or potential breach, regarding the processing of personal data within the City & Guilds Group, that person must immediately notify the City & Guilds Group Data Protection Team by sending an email to gdpr@cityandguilds.com and calling **020 7294 3548**.

4.1. The Data Protection Team, and relevant members of personnel, shall act in accordance with the action protocol set out below.

5. City & Guilds Group as Data Controller

5.1. Where the breach affects personal data that a member of the City & Guilds Group processes as data controller (ie it determines the purposes and means of the processing of personal data) the Data Protection Team, with the full co-operation of relevant personnel, shall comply with the formalities and procedures described in this section 5.

5.2. The Data Protection Team may require the member of personnel who has notified a personal data breach to immediately provide further information, to clarify any issue regarding the personal data breach, and to fully support the Data Protection Team's investigation into and notification of the breach or suspected breach.

5.3. Once a personal data breach notification has been received by the Data Protection Team, it shall coordinate with City & Guilds Group IT to immediately implement appropriate security measures aimed at neutralising the effects of the personal data breach. City & Guilds Group IT shall implement such measures as soon as possible, assisting the Data Protection Team when making decisions.

5.4. The Data Protection Team shall evaluate, as soon as possible, whether the personal data breach entails a risk to the rights and freedoms of the data subjects and, in such case, if that risk is high.

5.5. In order to determine whether a risk is high, the Data Protection Team shall consider the following: the type of breach; the nature, sensitivity and volume of personal data; the ease of identification of individuals; the severity of consequences for individuals; the special characteristics of data subjects affected (e.g. if they are children, disabled persons, etc.); the number of affected data subjects and the special characteristics of the City & Guilds Group, where relevant. For example, personal data breaches of unintelligible or encrypted information are also not considered to be high-risk.

5.6. If the Data Protection Team concludes that the personal data breach entails a risk for the

rights and freedoms of individuals, he or she shall notify the data breach to the Information Commissioner's Office ("**ICO**") within 72 hours from the time of discovery of the personal data breach.

5.7. If this time limit is not observed, the notice shall include the reasons why the notification was not sent on time. Any additional information discovered subsequently shall also be provided to the ICO without undue delay.

5.8. The Data Protection Team may notify the ICO of the data breach by:

5.8.1. By calling the ICO helpline (0303 123 1113). The normal opening hours of the ICO are Monday to Friday between 9am and 5pm. However, they are closed after 1pm on Wednesdays for staff training. When a person calls the ICO, the ICO will record the details of the breach and give the person advice about what to do next. The ICO may ask the following questions:

a) what has happened;

b) when and how the City & Guilds Group found out about the breach;

c) the people that have been or may be affected by the breach;

d) what the City & Guilds Group is doing as a result of the breach; and

e) who they should contact if they need more information and who else the City & Guilds Group has told.

5.8.2. Reporting the data breach online. This option may be more appropriate if the Data Protection Team is still investigating the personal data breach, and will be able to provide more information at a later date.

5.9. If the Data Protection Team considers that the risk to the rights and freedoms of individuals derived from the data protection breach is high, he or she shall draft a written notice addressed to the data subjects affected, and send it without undue delay to the data subjects whose personal data have been affected by the personal data breach, provided that such notice shall not be necessary in the following circumstances:

5.9.1. before the personal data breach occurred, the City & Guilds Group had already implemented appropriate technical and organisational measures regarding the personal data affected by the breach (particularly, measures aimed at making the data unintelligible for unauthorised persons; e.g. by encrypting the data).

5.9.2. after the personal data breach, the City & Guilds Group took measures aimed at ensuring that the risks to the rights and freedoms of the data subjects would not materialise;

5.9.3. the notice involves disproportionate effort. In this case, it shall be necessary to report the personal data breach by means of a public notification or equivalent.

5.10. The Data Protection Team shall keep a record of personal data breaches, including, amongst other matters, information regarding their effects and the implemented corrective

measures. For such purpose, the Data Protection Team shall take into account any available information, information provided by City & Guilds Group IT and information provided by the staff member who reported the personal data breach. These records shall be duly kept by the Data Protection Team.

5.11. The ICO may request additional information regarding any personal data breach. In such cases, the Data Protection Team shall provide this information accordingly with the full co-operation of the relevant members of the City & Guilds Group.

6. The City & Guilds Group as Data Processor

6.1. Where the data breach affects personal data that a member of the City & Guilds Group processes as data processor (e.g as it is processing personal data as part of a service to a third party) the Data Protection Team, with the full co-operation of relevant personnel, shall comply with the formalities and procedures described in this section 6.

6.2. In the event that a member of the City & Guilds Group detects or somehow discovers a breach regarding personal data that the member processes on behalf of a data controller, it shall notify the data controller without undue delay and, in any event, in line with the deadlines and procedures contractually agreed with the data controller.

6.3. Where a data controller has delegated personal data breach notification obligations to a member of the City & Guilds Group, that member shall act in accordance with section 5 (above) and/or as established in the relevant contract.

7. Compliance with this Policy

7.1. This policy does not form part of any employment contract, and may be amended at any time. However, any personnel who breach this policy may face disciplinary action, in accordance with applicable HR policies and procedures.