UK COLLEGE
OF BUSINESS AND COMPUTING

General Data Protection Regulation Policy 2018

Reviewed by	Larry Gall, Alexandra Willis
Reviewed on	18/05/18
Approved by	Academic Standards and Quality Committee
Approved	
Next reviewed by	May 2019
Version	V 5.0

Amendment Record

Date	Issue No.	Section/Page	Details of Change	Authorised By:
10/11/17	1.0	ALL	General review and update of total policy.	
18/05/18	2.0	ALL	Updated policy from Data Protection to General Data Protection Regulation 2018	

1. **Introduction**

1.1 This document explains The General Data Protection regulation (GDPR) and its impact on staff and learners at UKCBC. But any other relevant legislation in jurisdictions in which the College operates when processing personal data. The College takes its responsibilities about the management of the requirements of the General Data Protection Regulations 2018 and other Data Protection legislation seriously, and any infringement may be considered under disciplinary procedures.

2. **Scope**

2.1 The document covers the collecting, handling and removal of personal data that is obtained about individuals. As a whole, it forms a policy that should be followed and enforced by all staff members dealing with learner, Staff and client data. The College needs to process information about its employees, its students and other individuals: for example, to allow it to monitor performance, achievements and health and safety, and so that staff can be recruited and paid, courses organised and legal obligations (e.g. to funding bodies and the government) fulfilled. Such information must be collected and used fairly, stored safely and not disclosed unlawfully.

3. Definitions

3.1 Data - means information which –

a) is being processed by means of equipment operating automatically in response to instructions given for that purpose,
b) is recorded with the intention that it should be processed by means of such equipment,
c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,
d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record, or
e) is recorded information held by a public authority and does not fall within any of paragraphs (a) to (d).

3.2 Data controller – means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

3.3 Data Protection Officer (DPO) / Human Resources – Person in charge of ensuring that the collection, processing and destruction of data within the college meets guidelines stated by the General Data Protection Regulation 2018.

3.4 General Data Protection Regulation - General Data Protection Regulation (2018) is a regulation that Parliament and the ICO governs relating to the collection, retention, use and transmission of information about living individuals and the rights those individuals have to see this information.

3.5 GDPR Code of Practice – The code explains how the GDPR applies to the sharing of personal data. It provides practical advice to all organisation, whether public, private or third sector, that share personal data and covers systematic data sharing arrangements as well as ad hoc or one-off requests to share personal data.

3.6 GDPR Principles – The Principles define the conditions under which personal data is handled.

3.7 Data subject means an individual who is the subject of personal data.

3.8 Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

3.9 European Economic Area - The European Economic Area (EEA) comprises the countries of the European Union (EU), plus Iceland, Liechtenstein and Norway

3.10 European Union - The European Union is composed of 28 sovereign member states: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Croatia and the United Kingdom.

3.11 Individual – A single human being as distinct from a group, class, or family.

3.12 Organisation - a person or group of people intentionally organized to accomplish an overall, common goal or set of goals

3.13 Personal data – means data which relate to a living individual who can be identified
a) from those data, or
b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive data – is personal data that relates to a specific set of 'Special Categories' these categories must be treated with extra security these categories are:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Genetic data; and
- Biometric data (where processed to uniquely identify someone).

Sensitive data should be stored separately from other data in a secure, locked drawer or cabinet.

3.14 Processing, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including -
a) organisation, adaptation or alteration of the information or data,
b) retrieval, consultation or use of the information or data,
c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) alignment, combination, blocking, erasure or destruction of the information or data.

3.15 Relevant filing system - is defined in the Act as any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

3.16 Third Parties -, in relation to personal data, means any person other than –
a) the data subject,
b) the data controller, or
c) any data processor or other person authorised to process data for the data controller or processor.

4. **GDPR**

4.1 The General Data Protection Regulations (2018) and came in to force on 25 May 2018. GDPR has superseded The Data Protection Act 1998 which came into force on 1 March 2000. The purpose of GDPR is ensure that organisation are protecting EU Citizens data and not using it Irresponsibly. The Regulation governs the collection, retention, use and transmission of information about living individuals and the rights those individuals have to see this information. The Act covers personal information in both electronic form and manual form (e.g. paper files, card indices) if the information is held in a relevant, structured filing system.

4.2 UKCBC is a registered member of the Information Commissioner's Office (ICO), our registration number is Z3548994. Stringent processes are in place to ensure that we adhere to the principles of the General Data Protection Regulation and are able to deal with breaches if and when they occur. We are required to maintain certain personal data about individuals for the purposes of satisfying our operational and legal obligations.

5**.** **Data Protection Officer (DPO)**

5.1 The College will nominate an appropriate person as the College's Data Protection Officer, who will be a person of sufficient knowledge and seniority in the College.

5.2 The College will ensure that the identity of the College's Data Protection Officer is to be made known to all staff, students, contractors and volunteers and will also draw to their attention this Policy and associated documentation. The Data Protection Officer is responsible for drawing up guidance and promoting compliance with this policy.

5.3 The Data Protection Officer will have access to all relevant documents relating to legal compliance under General Data Protection Regulation (2018) and it is the Data Protection Officer (in consultation, when necessary, with the relevant senior officers) that will make the decisions regarding what information is released or exempted.

6. **What Does the Act Mean for Staff?**

6.1 All members of staff at UKCBC who handle or process personal data about individuals in any way (names, contact details, financial details, course details, personal circumstances, beliefs, etc.) must be aware of the GDPR Principles and how to apply them lawfully.

6.2 If you receive a request from an Individual or Organisation to gain access to Personal Data held by the College, in all cases DO NOT provide the data yourself.

6.3 Staff must ensure that:

- all personal information entrusted to them in the course of their employment is kept securely;
- no personal information is disclosed either verbally or in writing, unknowingly or otherwise to any unauthorised third party.
- no personal information is accessed by staff for any reason other than for legitimate college business
- any information that they provide to the college in connection with their own employment is accurate and up to date and that they inform the college of any changes in circumstances.

6.4 When members of staff are responsible for supervising students doing work which involves the processing of personal information (e.g. in research projects), they must ensure that those students are aware of the general Data Protection Regulations Principles and, in particular, the requirement to obtain the data subject's consent where appropriate.

Staff who are unsure about who are the authorised third parties to whom they can legitimately disclose personal data should seek advice from their line manager or the DPO.

6.5 If the individual wanting to gain access to the data is the subject of the data (i.e. Joe Bloggs wants to see his personal file), please refer the request to the Data Protection Officer/ HR, who will process the data subject access request.

6.6 Staff members involved in processing new types of Personal Data have a responsibility to inform the DPO/ HR so the College's notification can be immediately updated. In providing any such updates, full details should be included of the type of personal data to be processed (i.e. financial details, contact details, etc), who the subject of the data is (learners, staff, the public, etc), why the data is being processed (marketing, staff administration, etc) and whether the intention is at any time to transfer the data to a third-party external to the College who is not the subject of the data, including whether this is an international partner.

7. **What Does the Act Mean for Learners?**

7.1 All learners at the College who handle or process personal data about individuals (names, contact details, financial details, course details, personal circumstances, beliefs etc) in the

course of their studies must be aware of the GDPR Principles and how to apply them lawfully within the confines of the College General Data Protection Regulation policy.

8. **How Do I Make a Request for Personal Information Held About Me?**

8.1 To request personal information you must first fill in a "Subject Access Request" form. This form can be obtained from UK College of Business and Computing, Wentworth House, 350 Eastern Avenue, Gants Hill, Ilford. Essex IG2 6NW. The College will respond to all such requests as quickly as possible, but will ensure that it is provided within 30 calendar days as set out by the General Data Protection Regulations.

8.2 Individuals will not be entitled to access information to which any exemptions apply (e.g. when the information disclosed relates to more than one individual). However, only those specific pieces of information to which the exemption applies will be withheld, and information covered by an exemption will be subject to review by the DPO.

8.3 The College may charge any appropriate fee (£10) allowed for by General Data Protection Regulation should an individual request be manifestly unfound, excessive or if an individual request further copies following a prior request.

8.4 Where there is a data breach Staff and Students should refer to UKCBC GDPR Breach Procedure. Any significant breaches should be reported to the DPO, who in turn will be responsible for reporting the breach to the ICO in line with the requirements set out in the General Data Protection Regulation (2018).

9. **Data Protection Principles**

The principles state that personal information shall be:

9.1 Fairly and lawfully processed - in particular that the individual whose information it is has consented to the processing of his/her personal information.

9.2 Processed for limited purposes - only for the purposes for which it was originally supplied. College departments receiving personal information from individuals are obliged to ensure such individuals are fully aware of what we will use this information for. Staff should NOT assume that the provision of personal information gives the College the right to use that information for any purpose.

9.3 Adequate, relevant and not excessive - Data collected must be enough to complete the required task and no more.

9.4 Accurate and up to date – Where relevant Data should be kept up to date. Take reasonable action to ensure the accuracy of any Personal Data.

9.5 Not kept longer than is necessary - personal information should only be retained by the College for as long as is required to fulfil the purposes for which it was originally provided or required by law to be held. Beyond this point it should be securely destroyed.

9.6 Processed in accordance with the data subjects' rights - not to do anything with the information which would prejudice the rights of the individual in any way.

9.7 Secure - from the point at which personal information is received until the point at which it is destroyed, such information must be processed securely. College departments are obliged to ensure they have appropriate mechanisms in place to ensure adequate security for the storage and transmission of all electronic and paper records containing personal information, particularly more sensitive personal information. To avoid loss of information, all information has to be backed up securely and cannot be destroyed or disclosed until signed off by department heads or the DPO. Failure to comply with these guidelines would result in a breach of contractual obligation.

9.8 Not transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures an adequate level of protection (if you need to transfer data in this way, please consult the DPO /HR.

Staff, learners and members of the College must comply with the data protection principles.

10. FAQ

10.1 What if I get a request for personal data from an individual/organisation who isn't the subject of the data?

Personal data must NEVER be disclosed to unauthorised Third Parties (including family members) unless the data subject consents to the disclosure in writing or the disclosure:

- is necessary to protect the vital interests of the data subject (e.g. where failure could result in harm or death);
- is necessary to prevent serious harm to a third party;
- is necessary for national security
- is necessary for the prevention of crime or prosecution of offenders;
- is necessary for the assessment/collection of taxes or duty;
- is necessary for the discharge of regulatory functions including securing the health, safety and welfare of persons at work
- is required by legislation, by rule of law or by order of the court.
- is used for research purposes, subject to the specific rules shown under the heading 'Use of Personal Data in Research', below.

However, if a request for information is made from a third party under one of the points above, or if you are otherwise unsure how to handle a request for personal information, please contact the College's DPO/HR. Failure to deal with such a request appropriately can prejudice the interests of data subjects and result in action being taken against the College.

It is important to note that consent cannot be inferred from silence, therefore if consent from the subject is sought but no reply is received, then the information cannot be released.

10.2 **Does the Act allow access to examination documentation?**

Under the Act examination scripts are exempted from subject access rules. This means the College is under no obligation to permit candidates to have access to their original or copies of their original scripts. In addition to scripts any assessed work, assignments or field work would be deemed equivalent to examination scripts.

10.3 **Examination Marks**

It is the College practice to allow departments to release the breakdown of examination marks after the examination results have been published by the relevant examination board. However, in the event that a request is made by a candidate for details regarding their marks before results are formally announced the College is permitted to withhold the marks for 5 months from the date of the request. Under the rules of the Act the College is also permitted, if need be, to withhold marks for a maximum of 40 days from the announcement of the result. Note that such action would be unusual and would need the approval of the Chair of the examination board.

10.4 **Can individuals gain access to references about them?**

Confidential references provided by staff employed by the College are exempted from subject access requests where they relate to education, training, or employment of the data subject. Confidential references received by the College are not exempted from subject access requests and data subjects have the right to request a copy of the reference. However, in such circumstances the referee will be approached by the College first to give them the opportunity to object to the release of the documentation. The College wants all referees to be able to express their views frankly and without prejudice to themselves, so under no circumstances shall information contained within references be released to the data subject if it is the judgment of the DPO/HR that to do so would be prejudicial or harmful to the interests of the referee.

10.5 **How does The Act apply to Closed Circuit Television?**

The College complies with the Code of Practice for CCTV used to monitor areas where the public have access. For further details, please refer to the College's CCTV Usage Policy

10.6 **What should I be aware of when publishing information on the Internet?**

Important consideration needs to be given when presenting data on the web as, unless appropriate security is in place, the data is available beyond the EEA and therefore may contravene the Act. Personal data which is used for purposes such as normal operation of the College and is already available in publicly available hard copy may be published on the web without the data subjects consent; although they should be informed.

If personal data is to be published on the web which clearly identifies an individual, staff should ensure that consent has been given by the data subject and that adequate security is in place. If a subject refuses permission data should not be published on the web.
Staff authorised through the terms of their employment have the right to access, process and disclose personal data held on institutional computer systems where this is required within normal operations of the College.

10.7 What should I consider when taking photographs/videos of individuals?

Photographs and video images may be personal data as defined by the General Data Protection Regulations. The guiding principle is that images that allow identification of living individual(s)

will usually be classed as personal data and as such must be processed in line with the Data Protection Principles.

Images which are likely to be regarded as personal data:

- Photographs of individuals stored with personal details e.g. for ID cards
- Photographs of staff or learners published on departmental notice boards
- Photographs or videos of individuals or small groups used for marketing purposes

Images which are unlikely be regarded as personal data:

- Photographs of deceased individuals
- Photographs or videos of crowds or large events where individuals are included incidentally in the background and are not the focus of the image
- Photographs taken for purely domestic purposes are exempt from GDPR

Where an image constitutes personal data, it is important to ensure that data subjects (the people appearing in the image, this includes Audio recording and Testimonials) provide consent to the use of their image. For individuals and small groups, the Photograph and Video Permission Form can be used. For larger groups and events, it may be impractical to obtain written consent from all participants. However, it will be necessary to inform individuals that their image will be taken and provide them the opportunity to opt-out of their image being captured by removing themselves from the area. This can be done by way of verbal announcement(s) or ensuring there are clear signs around the venue.

When obtaining consent, you should inform individuals how their images will be used. Images cannot be used for additional purposes without obtaining relevant consent. For example, images collected for the purpose of maintaining departmental record of learners should not be published on the web without obtaining additional consent.

As with the collection of any personal data, consideration should be given to the length of time data will be held and the security requirements involved with processing.

Related Policies

- CCTV Usage Policy
- Data Retention Policy