Retention and Destruction Policy (GDPR)

Owner:	***Data Protection Officer***
Approved on:	***23 October 2018***
Review Date:	***February 2021***
Approved by:	***Senior Leadership Team***
Version No:	***1.2***

TABLE OF CONTENTS

1. OVERVIEW

The Hull College Group needs to collect, store and process personal data in order to carry out its functions and activities as a college. There are many reasons why we need to collect information including Safeguarding, for Health and Safety, to draw down funding for learners, to take fee payments or pay bursaries, or monitoring learning activity are just a few of these reasons. However all staff members within the Hull College Group are committed to protecting the confidentiality and integrity of the personal information it collects in line with the new GDPR legislation.

Under data protection law we have to provide details of how our organisation handles personal data about staff or customers, for the data protection register.

As an organisation that collects, uses and stores Personal Data about its employees, learners, suppliers, partners, governors, parents and visitors, the College recognises that having controls around the collection, use, retention and destruction of Personal Data is important to comply with the College's obligations under Data Protection Laws and in particular its obligations under Article 5 of GDPR.

The College has implemented this Retention and Destruction Policy to ensure all College Personnel are aware of the procedures for retaining and destroying personal data confidentially, as well as managers taking responsibility for ensuring their retention periods are up to date and appropriate,

College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any member of the College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All members of College Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact our Data Protection Officer, who is responsible for ensuring the College's compliance with this Policy.

2. ABOUT THIS POLICY

This Policy explains how the College complies with its legal obligation not to keep personal data for longer than is necessary and sets out when different types of personal data will be deleted. Data Protection Laws require that the College does not keep Personal Data longer than is necessary for the purpose, or purposes, for which the College collected it. In particular, it sets out details of the College's policies for the retention of Special Category personal data.

The Policy applies to all Personal Data stored in college systems, electronically, in paper form, or otherwise.

2.1. Hull College Group (the "**College**") must, in respect of its processing of personal data, comply with the Data Protection Act 2018, the General Data Protection Regulation 2016/679, and related legislation (together, "**Data Protection Laws**").

2.2. This Retention Policy should be read in conjunction with the College's Data Protection Policy, which sets out the College's overall approach to data protection matters and sets out the rationale for why a Retention Policy is required for personal data. It should also be read in conjunction with other policies such as; Acceptable use, Network Security and Information Security policies available on the internal portal.

2.3. The College is under a legal obligation only to keep personal data for as long as the College needs it. Once the College no longer needs personal data, the College must securely delete it.

2.4. This Policy applies to all College employees, consultants, contractors and temporary personnel hired to work on behalf of the College ("**College Personnel**").

2.5. All College Personnel with access to personal data must comply with this Retention Policy at all times whilst in college employment.

2.6. College Personnel are advised that the retention periods for information assets applies to all forms of media and storage.

2.7. You are advised that any breach of this Retention Policy will be treated seriously and may result in disciplinary action being taken against you.

2.8. Definitions are the same as set out in the Data Protection Policy

3. MAINTAINING THE INFORMATION ASSET REGISTER

Maintaining an up to date Information Asset Register acts as a central record of all the data assets the college holds, and enables the college to destroy records appropriately.

3.1. The College has assessed the types of personal data it holds and the purposes for why the data has been collected. All personal data collected by the college is set out in the College **Information Asset Register ("IAR")**.

3.2. The Data Protection Officer reviews all retention periods annually prior to approval of the policy. However, the IAR is a live document and will be updated in year subject to new information being collected or if retention periods change.

3.3. The IAR details all information collected by the College across the delivery areas of 14-16, Further Education, HE, Apprenticeships and our Childcare settings. It also details any information collected, processed and stored within the support and business functions of the college, detailing all the different types of personal data that each area holds. Each Information Asset is assigned an owner even if it is used across multiple teams.

3.4. The retention periods for all personal information collected are detailed specifically in relation to the purpose that piece of information was collected for, the lawful basis used for processing, the owner of the information, and agreed operational activity undertaken. The IAR also details the privacy notices in place for processing, any Data Protection Impact Assessments (DPIA) that have been done, and any special category information approved for collection.

3.5. The retention periods given in the IAR are subject to an additional 6-month period to allow for in year data cleansing points that ensure secure disposal of the information.

3.6. Any Data Sharing Agreements, or contractual requirements to share data with third parties, are also detailed in the register; including both within and outside the UK.

3.7. The register also outlines the special category data that the college must collect to meet government requirements and the safeguarding duties imposed on it.

3.8. If any member of College Personnel considers that a particular piece of personal data needs to be kept for more or less time than the period set out in this policy, they should contact the Data Protection Officer for guidance.

3.9. The College Privacy Notices give generic retention periods as it would be impossible to outline all the individual retention periods for all assets the college holds and still keep the notices simple and in a manageable size. The College Information Asset Register details all of the retention and destruction periods as set out by the individual processing laws or by the senior managers that control the use of that data.

For information on the IAR please contact the Data Protection officer on GDPR-Request@Hull-College.ac.uk

4. DATA SHARING AGREEMENTS WITH THIRD PARTIES

The college has to share information with third parties as detailed in the Privacy Notices, and this is done as outlined in our contractual arrangements or data sharing agreements.

If a requirement to share data is identified for a permitted purpose any processing of that data must be done in accordance with the terms set out in the college data sharing agreement. The agreement will detail what personal data can be shared and when, which groups of individuals are included in the dataset, and how long the third party can retain the data for.

4.1. The parties also agree certain technical and organisational measures to ensure that the shared Personal Data, is shared in a secure manner, and protected against accidental, unauthorised or unlawful destruction, loss, alteration, disclosure or access.

4.2. The Third party cannot permit any processing of Protected Data by any agent, subcontractor or other third party without the prior specific written authorisation of the College.

4.3. The Third party is bound by the agreement to only allow authorised staff access to the Protected Data. They have a duty to ensure those staff are adequately trained and have a binding and enforceable written contractual obligation to keep the Protected Data confidential.

4.4. The Third party cannot process and/or transfer, or otherwise directly or indirectly disclose, any Protected Data in or to countries outside the EU or EEA without the prior written consent of the College.

4.5. The Third party is governed by the same breach procedures as the college and is required to report any breach without undue delay.

The college does not consider that it transfers personal data outside the EEA, or any country where appropriate adequacy measures are not in place. This applies to our own personal data storage, or any company we use that are based overseas or their storage facilities are based overseas.

The college ensures it continually reviews its own processes and the compliance of its partners or contractors to ensure that we would be aware if any data transfers outside the EEA were required.

5 CHANGES TO THIS POLICY

The College reserves the right to change or update this policy at any time.