Data Protection Policy

Writtle University College
Lordship Road, Chelmsford
Essex, CM1 3RR

Tel: +44 (0)1245 424200
Fax: +44 (0)1245 420456
Email: info@writtle.ac.uk
www.writtle.ac.uk

Policy Owner	Department
University College Secretary	Professional Support
Version Number	**Date drafted/Date of review**
2.0	23 May 2018
Date Equality Impact Assessed	**Has Prevent been considered (see Policies Guidance if unsure)**
23 May 2018	Yes
Reviewed and Approved by (see Policies Guidance for approval process)	**Date**
SLT Governors	4 July 2018 13 July 2018
Access (tick as appropriate)	
Public access (website) ☒ And/Or Internal access (MyWi) ☒	Staff and Student access ☒ Or Staff access only ☐

Policy Overview and Scope

Writtle University College ("WUC") needs to keep certain personal information about its staff, students, and other clients/customers for academic, administrative and commercial purposes and to meet its legal obligations to funding bodies and the government. WUC is committed to compliance with the data protection laws and, in particular, its obligations under Article 5 of the General Data Protection Regulation ("GDPR").

This policy applies to all staff and also to students who are engaged to carry out work for the University College or those who use Personal Data in dissertations or elsewhere as a part of their studies.

Policy and Procedure

1. Introduction

1.1 This Policy (and the other policies and documents referred to in it) sets out the basis on which WUC will collect and use Personal Data either where the University College collects it from individuals itself, or where it is provided to WUC by third parties. It also sets out rules on how WUC handles, uses, transfers and stores Personal Data.

1.2 It applies to all Personal Data stored electronically, in paper form, or otherwise.

1.3 Any breach of this policy will be taken seriously and may result in disciplinary procedures being instigated.

2. Definitions

2.1 **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data.

2.2 **Data Protection Laws** – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

2.3 **Data Protection Officer –** Our Data Protection Officer can be contacted at: 01245 424200 or dpo@writtle.ac.uk.

2.4 **EEA** – Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

2.5 **ICO** – the Information Commissioner's Office, the UK's data protection regulator.

2.6 **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the University College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include partnerships and sole traders.

2.7 **Personal Data** – Any information about an Individual (see definition above) which identifies them, or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context.

2.8 **Processor** – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction or on behalf of a Controller.

2.9 **Special Categories of Personal Data –** Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health, sexual life or sexual orientation and criminal record. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.

2.10 **University College** – Writtle University College (**WUC**), Lordship Road, Writtle, CM1 3RR.

2.11 **University College Personnel** – Any WUC employee, worker or contractor who accesses any of the University College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of WUC.

3. University College Personnel's General Obligations

3.1 All University College Personnel must comply with this policy.

3.2 University College Personnel must ensure that they keep confidential all Personal Data that they collect, store, use and come into contact with during the performance of their duties.

3.3 University College Personnel must not release or disclose any Personal Data:

3.3.1 outside the University College; or

3.3.2 inside the University College to University College Personnel not authorised to access the Personal Data,

without specific authorisation from their manager or the Data Protection Officer; this includes by phone calls or in emails.

3.4 University College Personnel must take all steps to ensure there is no unauthorised access to Personal Data whether by other University College Personnel who are not authorised to see such Personal Data or by people outside the University College.

3.5 University College Personnel should take particular care when processing Special Categories of Personal Data. Emails containing such data which are being sent externally should be encrypted, for example by password protecting. Emails containing non-sensitive data (for example name or contact details) do not need to be encrypted, except in the case where a large amount of data is being sent out (for example a spreadsheet containing the names of 50 individuals).

4. Data Protection Principles

4.1 When using Personal Data, Data Protection Laws require that the University College complies with the following principles. These principles require Personal Data to be:

4.1.1 processed lawfully, fairly and in a transparent manner;

4.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

4.1.3 adequate, relevant and limited to what is necessary for the purposes for which it is being processed;

4.1.4 accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate, or no longer required, is erased or rectified as soon as possible;

4.1.5 kept for no longer than is necessary for the purposes for which it is being processed; and

4.1.6 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.

4.2 These principles are considered in more detail in the remainder of this Policy.

4.3 In addition to complying with the above requirements the University College also has to demonstrate in writing that it complies with them. The University College has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the University College can demonstrate its compliance.

5. Lawful Use of Personal Data

5.1 In order to collect and/or use Personal Data lawfully the University College needs to be able to show that its use meets one of a number of legal grounds. These are:

- The data subject has given consent;
- The processing is required due to a contract
- It is necessary due to a legal obligation
- It is necessary to protect someone's vital interests (i.e. a life or death situation)
- It is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
- It is necessary for the legitimate interests of the controller or a third party.

5.2 In addition when the University College collects and/or uses Special Categories of Personal Data (see 2.9 above), the University College has to show that one of a number of additional conditions is met:

- The data subject has given explicit consent;
- The processing is necessary for the purposes of employment, social security and social protection law;
- The processing is necessary to protect someone's vital interests;
- The processing is carried out by a not-for-profit body;
- The processing is manifestly made public by the data subject;
- The processing is necessary for legal claims;
- The processing is necessary for reasons of substantial public interest;
- The processing is necessary for the purposes of medicine, the provision of health or social care or treatment or the management of health or social care systems and services;
- The processing is necessary for public health; or
- The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

5.3 The University College has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 5.1 and 5.2. If the University College changes how it uses Personal Data, the University College needs to update this record and may also need to notify Individuals about the change. If University College Personnel therefore intend to change how they use Personal Data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

6. Transparent Processing – Privacy Notices

6.1 Where the University College collects Personal Data directly from Individuals, the University College will inform them about how the University College uses their Personal Data. This is in a privacy notice. The University College's Privacy Notices can be found at http://writtle.ac.uk/Privacy-and-Cookies.

6.2 If the University College receives Personal Data about an Individual from other sources, the University College will provide the Individual with a privacy notice about how the University College will use their Personal Data. This will be provided as soon as reasonably possible and in any event within one month.

6.3 If the University College changes how it uses Personal Data, the University College may need to notify Individuals about the change. If University College Personnel intend to change how they use Personal Data they should notify the Data Protection Officer who will decide whether the intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

7. Data Quality

7.1 Data Protection Laws require that the University College only collects and processes Personal Data to the extent that it is required for the specific purpose(s) notified to the individual in a privacy notice (see paragraph 6 above) and as set out in the University College's record of how it uses Personal Data. The University College is also required to ensure that the Personal Data the University College holds is accurate and kept up to date.

7.2 All University College Personnel who collect and record Personal Data shall ensure that the Personal Data is recorded accurately, is kept up to date and shall also ensure that they limit the collection and recording of Personal Data to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used.

7.3 All University College Personnel who obtain Personal Data from sources outside the University College shall take reasonable steps to ensure that the Personal Data is recorded accurately, is up to date and limited to that which is adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. This does not require University College Personnel to independently check the Personal Data obtained.

7.4 In order to maintain the quality of Personal Data, all University College Personnel who access Personal Data shall ensure that they review, maintain and update it to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected and used. Please note that this does not apply to Personal Data which the University College must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

7.5 The University College recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws.

8. Personal Data Retention

8.1 Data Protection Laws require that the University College does not keep Personal Data longer than is necessary for the purpose or purposes for which the University College collected it.

8.2 The University College has assessed the types of Personal Data that it holds and the purposes it uses it for and has set retention periods for the different types of Personal Data processed

by the University College, the reasons for those retention periods and how the University College securely deletes Personal Data at the end of those periods. These are set out in the Records Retention Policy and Schedule which are available on the WUC website or on request from the Data Protection Officer.

8.3 If University College Personnel feel that a particular item of Personal Data needs to be kept for more or less time than the retention period set out in the Records Retention Policy and Schedule, for example because there is a requirement of law, or if University College Personnel have any questions about this Policy or the University College's Personal Data retention practices, they should contact the Data Protection Officer for guidance.

9. Data Security

The University College takes information security very seriously and the University College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. The University College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

10. Data Breach

10.1 Whilst the University College takes information security very seriously, unfortunately, in today's environment, it is possible that a security breach could happen which may result in the unauthorised loss of, access to, deletion of or alteration of Personal Data. If this happens there will be a Personal Data breach and University College Personnel must comply with the University College's Data Breach Notification Policy. Please see paragraphs 10.2 and 10.3 for examples of what can be a Personal Data breach. Please familiarise yourself with it as it contains important obligations which University College Personnel need to comply with in the event of Personal Data breaches.

10.2 Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data. Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone does internally.

10.3 There are three main types of Personal Data breach which are as follows:

10.3.1 **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a University College Personnel is not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people "blagging" access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong student, or disclosing information over the phone to the wrong person;

10.3.2 **Availability breach** - where there is an accidental or unauthorised loss of access to, or destruction of, Personal Data e.g. loss of a memory stick, laptop or device, denial of service attack, infection of systems by ransom ware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from back up, or loss of an encryption key; and

10.3.3 **Integrity breach** - where there is an unauthorised or accidental alteration of Personal Data.

11. Appointing Contractors who access Personal Data

11.1 If the University College appoints a contractor who is a Processor of the University College's Personal Data, Data Protection Laws require that the University College only appoints them where the University College has carried out sufficient due diligence and only where the University College has appropriate contracts in place.

11.2 One requirement of GDPR is that a Controller must only use Processors who meet the requirements of the GDPR and protect the rights of individuals. This means that data protection due diligence should be undertaken on both new and existing suppliers. Once a Processor is appointed they should be audited periodically to ensure that they are meeting the requirements of their contract in relation to Data Protection.

11.3 Any contract where an organisation appoints a Processor must be in writing.

11.4 GDPR requires the contract with a Processor to contain the following obligations as a minimum:

11.4.1 to only act on the written instructions of the Controller;

11.4.2 to not export Personal Data without the Controller's instruction;

11.4.3 to ensure staff are subject to confidentiality obligations;

11.4.4 to take appropriate security measures;

11.4.5 to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;

11.4.6 to keep the Personal Data secure and assist the Controller to do so;

11.4.7 to assist with the notification of Data Breaches and Data Protection Impact Assessments;

11.4.8 to assist with subject access/individuals rights;

11.4.9 to delete/return all Personal Data as requested at the end of the contract;

11.4.10 to submit to audits and provide information about the processing; and

11.4.11 to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

11.5 In addition the contract should set out:

11.5.1 the subject-matter and duration of the processing;

11.5.2 the nature and purpose of the processing;

11.5.3 the type of Personal Data and categories of individuals; and

11.5.4 the obligations and rights of the Controller.

12. Individuals' Rights

12.1 GDPR gives individuals more control about how their data is collected and stored and what is done with it. Some existing rights of individuals have been expanded upon and some new rights have been introduced.

The different types of rights of individuals are reflected in this paragraph.

12.2 Subject Access Requests

Individuals have the right under the GDPR to ask a University College to confirm what Personal Data they hold in relation to them and provide them with the data.

12.3 Right of Erasure (Right to be Forgotten)

This is a limited right for individuals to request the erasure of Personal Data concerning them where:

12.3.1 the use of the Personal Data is no longer necessary;

12.3.2 their consent is withdrawn and there is no other legal ground for the processing;

12.3.3 the individual objects to the processing and there are no overriding legitimate grounds for the processing;

12.3.4 the Personal Data has been unlawfully processed; or

12.3.5 the Personal Data has to be erased for compliance with a legal obligation.

12.4 Right of Data Portability

An individual has the right to request that data concerning them is provided to them in a structured, commonly used and machine readable format where:

12.4.1 the processing is based on consent or on a contract; and

12.4.2 the processing is carried out by automated means

12.5 **The Right of Rectification and Restriction**

Individuals are given the right to request that any Personal Data is rectified if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

12.6 The University College will use all Personal Data in accordance with the rights given to Individuals' under Data Protection Laws, and will ensure that it allows Individuals to exercise their rights in accordance with the relevant policies.

13. Data Protection Impact Assessment (DPIA)

13.1 The GDPR introduce a new requirement to carry out a risk assessment in relation to the use of Personal Data for a new service, product or process. This must be done prior to the processing via a Data Protection Impact Assessment ("DPIA"). A DPIA should be started as early as practical in the design of processing operations. A DPIA is not a prohibition on using Personal Data but is an assessment of issues affecting Personal Data which need to be considered before a new product/service/process is rolled out. The process is designed to:

13.1.1 describe the collection and use of Personal Data;

13.1.2 assess its necessity and its proportionality in relation to the purposes;

13.1.3 assess the risks to the rights and freedoms of individuals; and

13.1.4 the measures to address the risks.

13.2 A DPIA must be completed where the use of Personal Data is likely to result in a high risk to the rights and freedoms of individuals. The ICO's standard DPIA template is available from www.ico.org.uk.

13.3 Where a DPIA reveals risks which are not appropriately mitigated the ICO must be consulted.

13.4 Where the University College is launching or proposing to adopt a new process, product or service which involves Personal Data, the University College needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The University College needs to carry out a DPIA at an early stage in the process so that the University College can identify and fix problems with its proposed new process, product or service at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

13.5 Situations where the University College may have to carry out a Data Protection Impact Assessment include the following (please note that this list is not exhaustive):

13.5.1 large scale and systematic use of Personal Data for the purposes of Automated Decision Making or Profiling (see definitions above) where legal or similarly significant decisions are made;

13.5.2 large scale use of Special Categories of Personal Data, or Personal Data relating to criminal convictions and offences e.g. the use of high volumes of health data; or

13.5.3 systematic monitoring of public areas on a large scale e.g. CCTV cameras.

13.6 All DPIAs must be reviewed and approved by the Data Protection Officer.

14. Transferring Personal Data to a Country outside the EEA

14.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. Transfer includes sending Personal Data outside the EEA but also includes storage of Personal Data or access to it outside the EEA. It needs to be thought about whenever the University College appoints a supplier outside the EEA or the University College appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

14.2 So that the University College can ensure it is compliant with Data Protection Laws University College Personnel must not export Personal Data unless it has been approved by the Data Protection Officer.

15. Registration with the Information Commissioner's Office

The official purposes for which WUC processes personal data must be notified to the Information Commissioner's Office annually. The University College's entry can be found at https://ico.org.uk/ESDWebPages/Entry/Z4944023.

16. Related Policies

The following policies are available at http://writtle.ac.uk/Policies-&-Procedures

- Research Ethics Policy
- Records Retention Policy and Schedule
- IS&T Usage Policy
- Data Breach Notification Policy

This policy supersedes any other policy and procedural guidelines, which may be in other existing University College documents. Writtle University College may amend this policy from time to time and any such amendments will be notified via the website, MyWi or by email.

If this information is difficult to access, read or understand, it can be provided in another format, for example in large print, or by someone talking it through with you.

Version Control

Version Number	Purpose/Amendment	Date
1.0	Existing policy moved onto WUC template	26 July 2016
1.1	Updates and re-write	12 October 2016
1.2	Update to HESA collection notice – new link	27 June 2017
2.0	GDPR version produced	25 May 2018