Data Protection Policy (UK GDPR)

Reference: GDPR/POL-1/DPO

Finance & Resources

1.	SLT approval	Date: 03.07.2020
2.	Governor approval	Date: 03.12.2020
3.	Equality Impact Assessment	Date: 23.06.2020
4.	Review due	Date: July 2024

TABLE OF CONTENTS **PAGE**

1. OVERVIEW

Warwickshire College Group's (**"WCG"**) reputation and future growth are dependent on the way it manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within WCG.

As an organisation that collects and processes Personal Data about its employees, suppliers (sole traders, partnerships or individuals within companies), students, governors, commercial clients, parents and visitors, WCG recognises that having controls around the collection, use, sharing, retention and destruction of Personal Data is important in order to comply with its obligations under Data Protection Laws and in particular its obligations under Article 5 of the UK GDPR.

WCG has implemented this Data Protection Policy to ensure all WCG Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data. This will maintain confidence in WCG and will provide for a successful working and learning environment for all.

WCG 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 WCG's Personnel's contract of employment and WCG reserves the right to change this Policy at any time. All members of WCG Personnel are obliged to comply with this Policy at all times.

If you have any queries concerning this Policy, please contact the Data Protection & Freedom of Information Officer (the DPO), who is responsible for ensuring WCG's compliance with this Policy. Contact details for the DPO are as follows:

- Email: dpo@wcg.ac.uk
- Telephone: 07858 300 228

2. ABOUT THIS POLICY

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

It applies to all Personal Data stored electronically and in paper form.

3. DEFINITIONS

3.1 **Warwickshire College (T/A Warwickshire College Group) known as "WCG"** – an organisation constituted under the Further & Higher Education Act 1992 as a charity and provider of further and higher education and training whose office for service is at Royal Leamington Spa College, Warwick New Road, Royal Leamington Spa, Warwickshire CV32 5JE.

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

3.3 **Controller** – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and process Personal Data. A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data that WCG is the Controller of includes: employee data, student data, contractor data, client

data. WCG will be viewed as a Controller of Personal Data if it decides what Personal Data it is going to collect and how it will use it. A common misconception is that individuals within organisations are the Data Controllers. This is not the case, it is the organisation itself which is the Controller.

3.4 **Data Breach** - see information under Clauses 11 and 12 of this Policy, the WCG Personal Data Breach Management Policy and the IT Security Incident Management Policy.

3.5 **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.

3.6 **Data Protection Officer** – Our Data Protection Officer is Lynda Cross, who can be contacted at: dpo@wcg.ac.uk or on 07858 300228.

3.7 **European Economic Area** ("**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.

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

3.9 **Individuals** – Living individuals who can be identified, directly or indirectly, from information that WCG 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, commercial clients and potential students. Individuals also include suppliers, partnerships and sole traders.

3.10 **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.

Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

WCG collects, stores and processes Ordinary Personal Data and Special Category Personal Data.

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

A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. Examples include: where software support for a system, which contains

Personal Data, is provided by someone outside the business; cloud arrangements; and mail fulfilment services.

3.12 **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.

4. WCG PERSONNEL GENERAL OBLIGATIONS

4.1 All WCG Personnel must comply with this policy.

4.2 WCG 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.

4.3 WCG Personnel must not release or disclose any Personal Data:
- 4.3.1 outside WCG; or
- 4.3.2 inside WCG to WCG 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.

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

5. DATA PROTECTION PRINCIPLES

5.1 When using Personal Data, Data Protection Laws require that WCG complies with the following principles. These principles require Personal Data to be:
- 5.1.1 processed lawfully, fairly and in a transparent manner;
- 5.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- 5.1.3 adequate, relevant and limited to what is necessary for the purposes for which it is being processed;
- 5.1.4 accurate and kept up to date, meaning that every reasonable step must be taken to ensure that Personal Data that is inaccurate is erased or rectified as soon as possible;
- 5.1.5 kept for no longer than is necessary for the purposes for which it is being processed; and
- 5.1.6 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.

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

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

demonstrate its compliance. The following policies and procedures underpin WCG's compliance:

a. Rights of Individuals Policy
b. Rights of Individuals Procedure
c. Personal Data Breach Notification Policy
d. IT Security Incident Management Policy
e. Data Breach Notification Procedure
f. Data Retention Policy
g. Data Retention Schedule
h. Email Retention Policy
i. Sensitive and Critical Information Policy
j. CCTV Access and Usage Policy
k. Appropriate Policy Document

6. LAWFUL USE OF PERSONAL DATA

6.1 In order to collect and/or process Personal Data lawfully WCG needs to be able to show that its use meets one of a number of legal grounds. Those legal grounds can be found on the website of the Information Commissioner's Office by clicking here.

6.2 In addition when WCG collects and/or processes Special Categories of Personal Data, it has to show that one of a number of additional conditions is met. Those conditions can be found on the website of the Information Commissioner's Office by clicking here.

6.3 WCG has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.1 and 6.2. If WCG changes how it uses Personal Data, it needs to update this record and may also need to notify Individuals about the change. If WCG Personnel therefore intend to change how they use Personal Data at any point they must notify theWCG Data Protection & Freedom of Information Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

6.4 WCG has recorded the types of Personal Data it collects and processes and the lawful basis of that processing in Appendix 1 to this Policy.

7. TRANSPARENT PROCESSING – PRIVACY NOTICES

7.1 Where WCG collects Personal Data directly from Individuals, it will inform them about how WCG uses their Personal Data. This is in a privacy notice or policy. WCG has adopted the following privacy notices:

- Privacy Policy (applicable to users of the WCG website and available here)
- Privacy Notice - Online Shop (applicable to online shopping at WCG from the intranet)
- Privacy Notice - Students/Apprentices (applicable to students and prospective students)
- Privacy Notice - Employees (applicable to WCG employees)
- Privacy Notice - Commercial letting of accommodation and/or classroom or office space
- Privacy Notice - Accommodation for enrolled students
- Privacy Notice - Conferencing facilities
- Privacy Notice - Online meetings (inc. meetings of the Corporation, staff meetings, tutorials, teaching delivery, etc)

7.2 If WCG changes how it uses Personal Data, it may need to notify Individuals about the change. If WCG Personnel therefore intend to change how they use Personal Data please notify the WCG Data Protection & Freedom of Information Officer who will decide whether WCG Personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

7.3 All WCG Privacy Notices are available on its Publication Scheme, unless they are being reviewed and updated..

8. DATA QUALITY – ENSURING THE USE OF ACCURATE, UP TO DATE AND RELEVANT PERSONAL DATA

8.1 Data Protection Laws require that WCG 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 7 above) and as set out in its record of how it uses Personal Data. WCG is also required to ensure that the Personal Data it holds is accurate and kept up to date.

8.2 All WCG Personnel that 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.

8.3 All WCG Personnel that obtain Personal Data from sources outside WCG 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 WCG Personnel to independently check the Personal Data obtained.

8.4 In order to maintain the quality of Personal Data, all WCG Personnel that 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 WCG must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.5 WCG recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. WCG has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how WCG responds to requests relating to these issues. Any request from an individual for the amendment, rectification, erasure or restriction of the use of their Personal Data should be dealt with in accordance with those documents.

9. PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

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

9.2 WCG 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 it, the reasons for those retention periods and how it securely deletes Personal Data at the end of those periods. These are set out in the Data Retention Policy.

9.3 If WCG 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 Data Retention Policy, for example because there is a requirement of law, or if WCG Personnel have any questions about this Policy or WCG's Personal Data retention practices, they should contact the Data Protection & Freedom of Information Officer for guidance.

10. DATA SECURITY

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

11. DATA BREACH

11.1 Whilst WCG 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 WCG Personnel must comply with WCG's Data Breach Notification Policy. Please see paragraphs 11.2 and 11.3 for examples of what can constitute a Personal Data breach. Please familiarise yourself with it as it contains important obligations which WCG Personnel need to comply with in the event of Personal Data breaches.

11.2 A 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 (or fails to do) within an organisation.

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

11.3.1 **Confidentiality breach** - where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that a WCG 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;

11.3.2 **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 ransomware, deleting Personal Data in error, loss of access to Personal Data stored on systems, inability to restore access to Personal Data from backup, or loss of an encryption key; and

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

11.4 The WCG Personal Data Breach Notification Policy provides further information.

12. IT SECURITY INCIDENT

12.1 An IT Security Incident is defined as:

"An event whereby any service or information stored or processed by WCG has been, or potentially has been, lost, destroyed, altered, copied, transmitted, stolen, used or accessed unlawfully or by unauthorised individuals accidentally or deliberately".

12.2 Where a security incident is reported to the Data Protection & Freedom of Information Officer, including a personal data breach, it will also be reported to WCG's IT Services for recording and any relevant action to be taken, if required.

12.3 The WCG IT Security Incident Management Policy provides further information.

13. APPOINTING CONTRACTORS WHO ACCESS PERSONAL DATA HELD BY WCG

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

13.2 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.

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

13.4 You are considered as having appointed a Processor where you engage someone to perform a service for you and as part of it they may get access to your Personal Data. Where you appoint a Processor you, as Controller, remain responsible for what happens to the Personal Data.

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

- 13.5.1 to only act on the written instructions of the Controller;
- 13.5.2 to not export Personal Data without the Controller's instruction;
- 13.5.3 to ensure staff are subject to confidentiality obligations;
- 13.5.4 to take appropriate security measures;
- 13.5.5 to only engage sub-processors with the prior consent (specific or general) of the Controller and under a written contract;
- 13.5.6 to keep the Personal Data secure and assist the Controller to do so;
- 13.5.7 to assist with the notification of Data Breaches and Data Protection Impact Assessments;
- 13.5.8 to assist with subject access/individuals rights;
- 13.5.9 to delete/return all Personal Data as requested at the end of the contract;
- 13.5.10 to submit to audits and provide information about the processing; and
- 13.5.11 to tell the Controller if any instruction is in breach of the GDPR or other EU or member state data protection law.

13.6 In addition the contract should set out:

- 13.6.1 the subject-matter and duration of the processing;
- 13.6.2 the nature and purpose of the processing;
- 13.6.3 the type of Personal Data and categories of individuals; and

13.6.4 the obligations and rights of the Controller.

14. INDIVIDUALS' RIGHTS

14.1 The GDPR gives individuals more control about how their data is collected and processed. Some existing rights of individuals have been expanded upon and some new rights have been introduced. It is extremely important that WCG plans how it will handle these requests in compliance with the UK GDPR.

14.2 The different types of rights that individuals benefit from under the UK GDPR are listed in paragraph 14.3 of this Policy. Further information can be obtained from the website of the Information Commissioner's Office by clicking here .

14.3 **Subject Access Requests**

14.3.1 Individuals have the right to be informed about the collection and use of their Personal Data. Subsequently, individual's have a right of access to their own Personal Data, known as a 'Subject Access Request'. This means that an individual can ask an organisation it believes is (or has been) processing their Personal Data what data it holds about them and why and to ask for a copy of that Personal Data. This is not a new right, but additional information has to be provided and the timescale for providing it has been reduced from 40 days to one month (with a possible extension if it is a complex request). An organisation cannot usually charge a fee for complying with a Subject Access Request. However, an organisation can charge a 'reasonable fee' for the administrative costs of complying with a request if it is manifestly unfounded or excessive, or if an individual requests further copies of their Personal Data.

14.3.2 Subject Access Requests are becoming more and more common and are often made in the context of a dispute which means that it is crucial that they are handled appropriately to avoid a complaint being made to the ICO.

14.4 **Right of Erasure (Right to be Forgotten)**

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

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

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

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

14.4.1.4 the Personal Data has been unlawfully processed; or

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

14.4.2 In a marketing context, where Personal Data is collected and processed for direct marketing purposes, the individual has a right to object to processing at any time. Where the individual objects, the Personal Data must not be processed for such purposes.

14.5 **Right of Data Portability**

14.5.1 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:

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

13.5.1.2 the processing is carried out by automated means

14.5.2 This right is not the same as subject access and is not a Subject Access Request. It is intended to give individuals a subset of their data.

14.6 **The Right of Rectification and Restriction**

14.6.1 Finally, individuals are also given the right to request that any Personal Data of theirs is rectified, if inaccurate and to have use of their Personal Data restricted to particular purposes in certain circumstances.

14.7 WCG 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 WCG's Rights of Individuals Policy and Rights of Individuals Procedure. Please familiarise yourself with these documents as they contain important obligations which WCG Personnel need to comply with in relation to the rights of Individuals over their Personal Data.

15. MARKETING AND CONSENT

15.1 WCG will sometimes contact Individuals to send them marketing or to promote WCG's courses and facilities. Where WCG carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

15.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. The UK GDPR will bring about a number of important changes for organisations that market to individuals, including:

15.2.1 providing more detail in their privacy notices, including for example whether profiling takes place; and

15.2.2 rules on obtaining consent will be stricter and will require an individual's "clear affirmative action". The ICO likes consent to be used in a marketing context.

15.3 Colleges also need to be aware of the Privacy and Electronic Communications Regulations (PECR) 2003 that sit alongside data protection. PECR applies to direct marketing i.e. a communication directed to particular individuals and covers any advertising/marketing material. It applies to electronic communication i.e. calls, emails, texts, faxes. PECR rules apply even if you are not processing any personal data

15.4 Consent is central to electronic marketing. We would recommend that best practice is to provide an un-ticked opt-in box.

15.5 Alternatively, WCG may be able to market using a "soft opt in" if the following conditions were met:

15.5.1 contact details have been obtained during the course of a sale (or negotiations for a sale) for goods or services;

15.5.2 WCG is marketing its own similar services; and

15.5.3 WCG gives the individual a simple opportunity to refuse to opt out of the marketing, both when first collecting the details and in every message after that.

16. AUTOMATED DECISION MAKING AND PROFILING

16.1 Under Data Protection Laws there are controls around profiling and automated decision making in relation to Individuals.

16.2 Automated Decision Making happens where WCG makes a decision about an Individual solely by automated means without any human involvement and the decision has legal or other significant effects; and

16.3 Profiling happens where WCG automatically uses Personal Data to evaluate certain things about an Individual.

16.4 Any Automated Decision Making or Profiling which WCG carries out can only be done once it is confident that it is complying with Data Protection Laws. If WCG Personnel therefore wish to carry out any Automated Decision Making or Profiling WCG Personnel must inform the Data Protection Officer.

16.5 WCG Personnel must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

16.6 WCG does not carry out solely Automated Decision Making or Profiling in relation to its employees.

17. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

17.1 The UK GDPR introduces 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:

17.1.1 describe the collection and use of Personal Data;
17.1.2 assess its necessity and its proportionality in relation to the purposes;
17.1.3 assess the risks to the rights and freedoms of individuals; and
17.1.4 the measures to address the risks.

17.2 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 its website here.

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

17.4 Where WCG is launching or proposing to adopt a new process, product or service which involves Personal Data, it needs to consider whether it needs to carry out a DPIA as part of the project initiation process. WCG needs to carry out a DPIA at an early stage in the process so that it 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.

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

17.5.1 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;
17.5.2 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

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

17.6 All DPIAs must be reviewed and approved by the WCG Data Protection & Freedom of Information Officer.

18. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

18.1 Data Protection Laws impose strict controls on Personal Data being transferred outside the EEA. A transfer includes sending Personal Data outside the EEA, but also includes storage of Personal Data or access to it outside the EEA. Transfers of Personal Data need to be thought through whenever WCG appoints a supplier outside the EEA or where WCG appoints a supplier with subsidiary companies within its group that are outside the EEA and which may give access to the Personal Data to staff outside the EEA.

18.2 So that WCG can ensure it is compliant with Data Protection Laws, WCG Personnel must not transfer or export Personal Data until they have consulted the Data Protection & Freedom of Information Officer.

18.3 WCG Personnel must not transfer or export any Personal Data outside the EEA without consulting the WCG Data Protection & Freedom of Information Officer.

APPENDIX 1

A. WCG processes the personal data of all students (FE and HE) and potential students at enquiry, application and enrolment stages. This is done under the lawful basis of performance of a contract that is or is intended to be in place between WCG and the individual for the purposes of delivering education, training, accommodation, meals and any other service or goods that the data subject is entitled to receive from WCG under the terms of business and/or syllabus of the course they have enrolled upon and where applicable. Personal data is also processed by WCG and its auditors in compliance with legal obligation as a statutory requirement for inspection and funding purposes as set out by the Department for Education (DfE), the Education & Skills Funding Agency (ESFA), the European Social Fund (ESF) and other funding and inspection bodies/agencies such as the Office for Standards in Education, Children's Services and Skills, known as 'Ofsted'.

B. WCG processes the personal data of Higher Education students for the purposes of sharing their name, date of birth and address with the Office for Students (OfS) and the Higher Education Statistics Agency (HESA). The OfS and HESA are statutory bodies which, amongst other services, conduct student surveys for the improvement of services and facilities offered to students by education providers. Examples of such surveys include the National Student Survey and the Graduate Outcomes survey. Personal Data is shared with these agencies under the lawful basis of public interest/exercise of official authority. It is in the public interest that minimal, but relevant personal data, is shared with these agencies to enable surveys to be conducted to bring about improvements to the Higher Education sector. As there are significant numbers of HE students enrolling on courses each year it would be logistically impossible to gather valid consent from each and every student. However, if students do not want their personal data to be shared with these agencies for the purpose of taking part in any survey they should contact the WCG Data Protection & Freedom of Information Officer on dpo@wcg.ac.uk and their wishes will be forwarded to WCG's HE department.

   WCG also shares the personal data of HE students and students applying for HE courses with the Universities and Colleges Admissions Service (UCAS). UCAS is an independent charity providing information, advice, and admissions services. The UCAS helps people figure out what the next step in their education might be and supports them in taking that step.

C. WCG processes the personal data of students, apprentices and delegates attending on commercial/business courses, e.g. customer services courses, management training courses, etc that have enrolled on a course, training programme and/or an apprenticeship, for the purpose of investigating and carrying out disciplinary proceedings against a data subject where, on the balance of probabilities, the data subject has contravened any WCG behavioural policy, protocol, strategy or code of practice or conduct. The lawful basis of this processing is the performance of a contract that is or is intended to be in place between WCG and the individual and the public interest/exercise of official authority. It is in the public interest and also in the interest of the data subject and others that disciplinary proceedings are implemented fairly to prevent poor and in some instances, criminal behaviour from getting out of hand and adversely affecting the behaviour and learning of other students.

D. WCG processes personal data of students, apprentices, staff and other visitors (invited and uninvited) on WCG premises using CCTV, as well as recording their personal data for the primary reasons of the teaching and learning contract with students /

apprentices, employment contract of employees and safeguarding children and vulnerable adults whilst they are on site. Where a person is suspected of committing, or is in the process of committing a criminal offence, whilst on WCG premises or against WCG property that evidence, along with other personal data WCG may hold about that individual, may be shared with the police for the purposes of criminal investigation, the prevention or detection of crime and the prosecution or apprehension of offenders. WCG may also process data captured on CCTV where necessary to protect the vital interests of a person. In some instances, where the allegation and evidence concerns the use, supply and/or sale of unlawful drugs on WCG premises, including WCG accommodation, WCG will inform the police and will cooperate with any police investigation, including the sharing of the personal data of those students reasonably believed to be involved. The lawful bases for processing personal data for this purpose, dependent on specific circumstances, are the legitimate interests of WCG and those of third parties, which includes WCG's commercial interests, individuals interests that have been affected, or are likely to be affected, or for the broader societal benefits. The processing is necessary and WCG cannot reasonably achieve the same result in another less intrusive way; to fulfil a civic duty to report crime in the public interest. The processing is necessary and WCG cannot reasonably achieve the same result in a less intrusive way; vital interests of the data subject themselves or another natural person to protect their life. WCG may also share personal data it holds The processing of personal data held by WCG in the act of sharing it with a recognised law enforcement body, local authority, council or other tax collection agency is exempt from certain UK GDPR provisions under Schedule 2, Part 1 of the Data Protection Act 2018. For more information please see paragraph E below.

E. Where the police and/or security services approach WCG for the personal data of individuals, e.g. staff and/or student personal data, for the purposes of criminal investigation, the prevention or detection of crime, the prosecution or apprehension of offenders and/or protecting the vital interests of a person, WCG will cooperate with such a request. The lawful bases of legal obligation and public interest/exercise of official authority will be relied on for the purposes of this processing, specifically:
   - Schedule 2 Part 1 Paragraph 2 of the Data Protection Act 2018 and GDPR Article 6(1)(d);
   - Part 3 Chapter 1 s.31 Data Protection Act 2018 - Law Enforcement purposes; and
   - Schedule 2 Part 1 s.2(1)(a) and (b) Data Protection Act 2018.

F. WCG processes the personal data of applicants for employment and of existing staff members for the proper performance of their contract of employment and under its legal obligation to comply with employment and equality legislation. WCG also processes the personal data of relevant employees in respect of statutory obligations to share CV and/or qualifications with awarding bodies and/or delivery partners and also under a legal obligation to comply with funding rules when benefitting from projects funded by the European Social Fund (ESF) and/or the European Regional Development Fund (ERDF). Employee salary details and payroll information will be shared with ESF and/or ERDF bodies to provide evidence of spend on projects for the proper claiming of funding.

G. WCG processes the Special Category personal data of students, apprentices, employees and visitors, although no person is obliged to disclose that data:
   - racial or ethnic origin
   - religious or philosophical beliefs
   - health

- sexual orientation

This data may be collected via the use of CCTV on WCG premises. CCTV is used for the safety and welfare of people on WCG premises as well for the protection of WCG premises and property (please see paragraphs D and E above). However, it is also collected to try and ensure WCG is able to support its students and employees in every way possible, especially where a student or employee requires support or reasonable adjustments put in place to assist them with a physical or mental health disability or difficulty or a learning difficulty. The lawful basis for this processing is the explicit consent of the individual, but in addition to this WCG has a legal obligation under the Equality Act 2010 and employment legislation in respect of employees, once informed of a disability, to implement support arrangements and/or reasonable adjustments.

H. WCG processes the Special Category personal data, specifically health data, of students and will share this data with a work placement provider where that student is enrolled on a course that requires them to undertake a work or industry placement in order to achieve the qualification they are studying. WCG will process this data and share the data with the relevant supervising manager at that work or industry placement where the physical disability or mental health, developmental, learning or behavioural difficulty may affect that work or industry placement and whether it is an appropriate or safe placement, based on the student's disclosure. The lawful authority that WCG will rely on, in the absence or refusal of the data subject's explicit consent, is legal obligation in order to comply with the Equality Act 2010 and the Health & Safety Act 1974; performance of a contract with the data subject in that the data subject must complete the work or industry placement as a fundamental part of their course; and the vital interests of the data subject should they suffer an episode of ill health or difficulty whilst undertaking the work or industry placement.

I. WCG processes ordinary personal data and Special Category personal data of students in respect of its Safeguarding duty under the Safeguarding Vulnerable Groups Act 2006, the Equality Act 2010, Health & Safety legislation and its duty of care under common law. This processing is also necessary for the performance of a task carried out in the public interest and in the exercise of official authority vested in WCG. WCG will process this data by sharing it with its insurance broker/company and/or the Health & Safety Executive (where necessary) in the event of an accident resulting in injury or an incident concerning other issues, as specified under 'The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013'. WCG also processes this data to protect the vital interests of the individual in situations where their, or another person's, life, health and welfare may be at risk as a result of a safeguarding or health and safety incident.

J. WCG processes the personal data of students and staff members as a result of UK Visa and Immigration legislation and national policy. On some courses this may require the taking of video footage and/or a photograph. WCG also processes the photographs and video footage of its staff, students, visitors, clients and contractors in the public interest and in the exercise of its official authority for the purpose of safeguarding and welfare of those on its premises. Photographs are used on WCG ID badges attached to colour specific lanyards and video footage of individuals on premises is recorded by static closed-circuit television cameras located around the college campuses.

K. WCG processes the personal data of its students, visitors and clients with their consent in respect of its marketing activities, e.g. for prospectuses, WCG's online presence, e.g. website, intranet, Facebook, Twitter.

Revision history

Dates of revision	Revised by	Description
07.05.2020	Lynda Cross, DPO	Conversion to AoC recommended policy.
02.12.2021	Lynda Cross, DPO	Inclusion of reference to IT Security Management Policy and definition of an IT Security Incident.
15.06.2022	Lynda Cross, DPO	Scheduled review for accuracy and updating.