Reaseheath Group Data Protection Policy

Table of Contents

1. OVERVIEW

The Group's reputation and future growth are dependent on the way the Group manages and protects Personal Data. Protecting the confidentiality and integrity of Personal Data is a key responsibility of everyone within the Group.

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

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

Group staff will be given access to a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not set terms or conditions of employment or form part of any Group contract of employment and Reaseheath College reserves the right to change this Policy at any time. All members of staff 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 Group's compliance with this Policy.

2. ABOUT THIS POLICY

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

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

This policy applies to all personal data we process regardless of the media in which that data is stored or whether it relates to past or present employees, students, contractors, customers, clients or supplier contacts, governors, website users or any other data subject.

This policy applies to all Group staff. All members of Staff must read, understand and comply with this policy when processing personal data on our behalf and attend/complete the training on its requirements. This privacy standard sets out what is expected from staff in order for the Group to comply with applicable law. Your compliance with this policy is mandatory. Related policies are available to help interpret and act in accordance with the policy. All related policies must also be complied with. Any breach of this policy may result in disciplinary action.

3. DEFINITIONS

3.1 Automated Decision-Making (ADM) – When a decision is made which is based solely on automated processing (Including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-making (unless certain conditions are met) but not Automated Processing.

3.2 **Automated Processing** – any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, location or movements. Profiling is an example of Automated Processing.

3.3 Reaseheath Group - comprised of Reaseheath College, Reaseheath University Centre, Burrows Lane Equestrian Centre and Croft End Equestrian Centre. The Main site is Reaseheath College Campus, Nantwich CW5 6DF.

3.4 **Group Staff** – Any Reaseheath Group employee, worker or contractor who accesses any of the Group's Personal Data and will include employees, consultants, contractors, and temporary staff hired to work on behalf of the Group.

3.5 **Consent** – agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

3.6 **Data Controller (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.

A Data Controller is responsible for compliance with Data Protection Laws and establishing practices and policies in line with the GDPR.

Example: The College is the Data Controller of all Personal Data relating to our College staff and Personal Data used in our business for our own commercial purposes.

A common misconception is that individuals within organisations are the Controllers. This is not the case it is the organisation itself which is the Controller.

3.7 **Data Protection Impact Assessment (DPIA)** – tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

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

A Data 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.

3.9 **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.

3.10 **Data Protection Officer –** the person required to be appointed in specific circumstances under the GDPR. When a mandatory DPO has not been appointed, this term means the data protection manager or other voluntary appointment of a DPO or refers to the Company data privacy team with responsibility for data protection compliance: Reaseheath Group Data Protection Officer is the Vice Principal Finance and Resources, and can be contacted at: 01270 613202, e-mail: DPO@reaseheath.ac.uk.

3.11 **Data subject** – Living individuals who can be identified, *directly or indirectly*, from information that the Group 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.

3.12 **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.

3.13 **Explicit Consent –** consent which requires a very clear and specific statement (that is, not just action).

3.14 **General Data Protection Regulation (GDPR) –** the General Data Protection Regulation (*(EU) 2016/679*). Personal Data is subject to the legal safeguards specified in the GDPR.

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

3.16 **Individuals** – Living individuals who can be identified, *directly or indirectly*, from information that the Group has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if anyone 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.

3.17 **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. Personal Data also includes Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviours.

3.18 **Personal Data Breach** – any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that the Group or our third-party service

providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

3.19 **Privacy Notices or Privacy Policies –** separate notices setting out information that may be provided to Data Subjects when the Group collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be standalone, one time privacy statements covering Processing related to specific purpose.

3.20 **Processing or Process –** any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

3.21 **Pseudonymisation of Pseudonymised –** replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

3.22 **Related Policies –** the Group's policies, operating procedures or processes related to this privacy notice and designed to protect personal data.

3.23 **Special Categories of Personal Data or Sensitive 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. REASEHEATH GROUP STAFF GENERAL OBLIGATIONS

4.1 All Group staff must comply with this policy.

4.2 Group staff 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 Group staff must not release or disclose any Personal Data:

4.3.1 outside the Reaseheath Group; or

4.3.2 inside the Group to Group staff 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 Group staff must take all steps to ensure there is no unauthorised access to Personal Data whether by other Group staff who are not authorised to see such Personal Data or by people outside the Group.

5. DATA PROTECTION PRINCIPLES

5.1 When using Personal Data, Data Protection Laws require that the Group complies with the following principles. These principles require Personal Data to be:

5.1.1 processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

5.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (Purpose Limitation);

5.1.3 adequate, relevant and limited to what is necessary for the purposes for which it is being processed (Data Minimisation);

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 (Accuracy);

5.1.5 not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is being processed (Storage Limitation);

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 (Security, Integrity and Confidentiality);

5.1.7 Not transferred to another country without appropriate safeguards being in place (Transfer Limitation);

5.1.8 Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests)

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, the Group also has to demonstrate in writing that it complies with them. The Group has a number of policies and procedures in place, including this Policy and the documentation referred to in it, to ensure that the Group can demonstrate its compliance. (Accountability)

6. LAWFUL USE OF PERSONAL DATA

6.1 Personal data must be processed lawfully, in a fair and transparent manner in relation to the data subject.

6.2 The Group may only collect, process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts actions regarding Personal Data to specified lawful

purposes. These restrictions are not intended to prevent Processing, but ensure that Personal Data is processed fairly and without adversely affecting the data subject.

6.3 In order to collect and/or use Personal Data lawfully the Group needs to be able to show that its use meets one of a number of legal grounds.

These are set out in Article 6 of the GDPR and are as follows:

- the Data Subject has given his or her consent;
- the processing is necessary for the performance of a contract with the Data Subject;
- the processing is necessary for compliance with a legal obligation to which the controller is subject;
- the processing is necessary in order to protect the vital interests of the individual or of another natural person;
- the processing is necessary for the performance of a task carried out in the public interest;
- the use of the Personal Data is for the purposes of the legitimate interests of the Controller.

Further information on detailed grounds can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

6.4 In addition when the Group collects and/or uses Special Categories of Personal Data, the Group has to show that one of a number of additional conditions is met.

These are set out in Article 9 and are as follows (paraphrased):

- explicit consent;
- employment and social security obligations;
- vital interests;
- necessary for establishment or defence of legal claims;
- substantial public interest; and
- various scientific and medical issues.

Further information on detailed additional conditions can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data

6.5 The Group has carefully assessed how it uses Personal Data and how it complies with the obligations set out in paragraphs 6.3 and 6.4. If the Group changes how it uses Personal Data, the Group needs to update this record and may also need to notify Individuals about the change. If Group staff intend, therefore, to change how they use Personal Dataat 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.

7. CONSENT

7.1 A Data Controller must only process Personal Data on the basis of one or more lawful basis set out in GDPR, which include Consent.

7.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters**.**

7.3 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may be needed to be refreshed if there is intention to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

7.4 Unless there is another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, Automated Decision-Making and for cross border data transfers. Usually the Group will be relying on another legal basis (and not require Explicit Consent) to process most types of Sensitive Data. Where Explicit Consent is required, a Privacy Notice to the Data Subject to capture Explicit Consent must be issued.

7.5 Consent needs to be evidenced records kept of all Consents so that the Group can demonstrate compliance with Consent requirements.

8. TRANSPARENT PROCESSING – PRIVACY NOTICES

8.1 The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate privacy notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

8.2 Where the Group collects Personal Data directly from Data Subjects, including for human resources or employment purposes, the Group must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and the DPO, how and why the Group will use, process, disclose, protect and retain that personal data through a Privacy Notice which must be presented when a data subject first provides the personal data. The Group has adopted the following Privacy Notices:

- Privacy Notice (Staff)
- Privacy Notice (Job Applicants)
- Privacy Notice (Applicants)
- Privacy Notice (Students)
- Privacy Notice (Website)
- Privacy Notice (Governors)

8.3 When Personal Data is collected indirectly (For example, from a third party or publicly available source), the Group must provide the Data subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. The Group must also check that the personal data was collected by the third-party in accordance with the GDPR.

8.4 If the Group changes how it uses Personal Data, the Group may need to notify Individuals about the change. If Group staff intend, therefore, to change how they use Personal Data

please 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.

9. DATA MINIMISATION

9.1 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

9.2 Personal data may only be processed when performing the job duties that require it. It cannot be processed for any reason not related to your job duties.

9.3 Personal Data may only be collected that is required for job duties: excessive data should not be collected. Ensure any Personal Data collected is adequate and relevant to the intended purposes.

9.4 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the Group's data retention guidelines.

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

10.1 Data Protection Laws require that the Group 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 8 above) and as set out in the Group's record of how it uses Personal Data. The Group is also required to ensure that the Personal Data the Group holds is accurate and kept up to date.

10.2 All Group Staff 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.

10.3 All Group Staff that obtain Personal Data from sources outside the Group 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 Group Staff to independently check the Personal Data obtained.

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

10.5 The Group recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. The Group has a Subject Access Policy and a Subject Access Procedure which set out how the Group 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.

11. STORAGE LIMITATION – PERSONAL DATA MUST NOT BE KEPT FOR LONGER THAN NEEDED

11.1 Data Protection Laws require that the Group does not keep Personal Data in an identifiable form longer than is necessary for the purpose or purposes for which the Group collected it.

11.2 Personal data must not be kept in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which it was originally collected including for the purpose of satisfying any legal, accounting all reporting requirements.

11.3 The Group 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 Group, the reasons for those retention periods and how the Group securely deletes Personal Data at the end of those periods. These are set out in the Reaseheath Group Records Retention Schedule.

11.4 The Group will ensure Data subjects are informed of the period for which data is stored and how that period is determined in any applicable privacy notice.

11.5 If Group Staff 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 Schedule, for example because there is a requirement of law, or if Group Staff have any questions about this schedule or the Group's records retention practices, they should contact the Data Protection Officer for guidance.

12. DATA SECURITY

12.1 Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

12.2 The Group takes information security very seriously and the Group has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data.

12.3 The Group will develop, implement and maintain safeguards appropriate to size, scope and business, and available resources, the amount of Personal Data owned or maintained on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). The Group will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. The Group has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

12.4 All are responsible for protecting the personal data the Group holds.

12.5 Staff must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against accidental loss of, or damage to, Personal Data.

12.6 Staff must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

12.7 Staff must maintain data security by protecting confidentiality, integrity and availability of the Personal Data, defined as follows:

12.7.1 **Confidentiality** means that only people who have a need to know and are authorised to use the Personal Data can access it.

12.7.2 **Integrity** means Personal Data is accurate and suitable for the purpose to which it is processed.

12.7.3 **Availability** means that authorised users are able to access Personal Data when they need it for authorised purposes.

12.8 Where appropriate, the security measures will be enforced and supported by the use of Group Policies and procedures including:

- Information Classification Policy
- Clear Desk and Screen Policy
- College Security Policy

12.9 Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Group implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

13. DATA BREACH

13.1 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulatory body and, in certain instances, the Data Subject.

13.2 Whilst the Group takes information security very seriously, however, 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 Staff must comply with the Incident Response Procedure. Paragraphs 13.4 and 13.5 demonstrate examples of what can be a Personal Data breach. Staff should familiarise themselves with it as it contains important obligations which Group Staff need to comply with in the event of Personal Data breaches.

13.3 If an individual knows or suspects that a Personal Data Breach has occurred, they should not attempt to investigate the matter. They should Immediately contact the DPO for further advice whilst preserving all evidence relating to the potential Personal Data Breach.

13.4 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 internal does.

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

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

13.5.2 **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 back up, or loss of an encryption key; and

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

14. APPOINTING CONTRACTORS WHO ACCESS THE GROUP'S PERSONAL DATA

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

14.2 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.

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

14.4 The Group is considered as having appointed a Processor when someone is engaged to perform a service for the Group and as part of it they may get access to Personal Data. Where the Group appoints a Processor, the Controller (the Group) remain responsible for what happens to the Personal Data.

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

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

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

14.5.3 to ensure staff are subject to confidentiality obligations;

14.5.4 to take appropriate security measures;

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

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

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

14.5.8 to assist with subject access/individuals rights;

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

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

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

14.6 In addition the contract should set out:

14.6.1 The subject-matter and duration of the processing;

14.6.2 the nature and purpose of the processing;

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

14.6.4 the obligations and rights of the Controller.

15. INDIVIDUALS' RIGHTS

15.1 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. It is extremely important that the Group considers how they will handle these requests under GDPR.

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

15.3 Subject Access Requests

15.3.1 Individuals have the right under the GDPR to ask a College to confirm what Personal Data they hold in relation to them and provide them with the data. This is not a new right but additional information has to be provided and the timescale for providing it is one month (with a possible extension if it is a complex request). In addition, it is no longer possible to charge a fee for complying with the request.

15.3.2 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.

15.4 Right of Erasure (Right to be Forgotten)

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

15.4.1.1 the use of the Personal Data is no longer necessary;
15.4.1.2 their consent is withdrawn and there is no other legal ground for the processing;
15.4.1.3 the individual objects to the processing and there are no overriding legitimate grounds for the processing;
15.4.1.4 the Personal Data has been unlawfully processed; and
15.4.1.5 the Personal Data has to be erased for compliance with a legal obligation.

15.4.2 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.

15.5 Right of Data Portability

15.5.1 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:

15.5.1.1 the processing is based on consent or on a contract; and
15.5.1.2 the processing is carried out by automated means

15.5.2 This right isn't the same as subject access and is intended to give individuals a subset of their data.

15.6 The Right of Rectification and Restriction

15.6.1 Finally, individuals are also 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.

15.7 The Group 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 Group's Subject Access Policy and Subject Access Procedure. These documents contain important obligations which Group Staff need to comply with in relation to the rights of Individuals over their Personal Data.

16. ACCOUNTABILITY

16.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance data protection principles. The Data Controller is responsible for, must be able to demonstrate, compliance with the data protection principles.

16.2 The Group must have adequate resources and controls in place to ensure and to document GDP compliance including:

16.2.1 appointing a suitably qualified DPO (where necessary) and an executive accountable for Data Privacy.

16.2.2 Implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high-risk to rights and freedoms of Data Subjects.

16.2.3 Integrating data protection into internal documents including this Data Protection Policy, Related Policies and Privacy Notices.

16.2.4 Regularly training Group Staff on the GDPR, this policy and related policies and data protection matters including, for example, Data Subject rights, Consent, legal basis, DPIA and Personal Data Breaches. The Group must maintain a record of training attendance by Group Staff; and

16.2.5 Regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

17. RECORDKEEPING

17.1 The GDPR requires the Group to keep full and accurate records of all data processing activities.

17.2 The Group must keep and maintain accurate corporate records reflecting processing including records of Data Subjects' Consents and procedures for obtaining Consents.

17.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO. Clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfer, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

18. TRAINING AND AUDIT

18.1 The Group are required to ensure all Group Staff have undergone adequate training to enable them to comply with Data Privacy. The Group must also regularly test its systems and processes to assess compliance.

18.2 All Group Staff must undergo all mandatory Data Privacy related training.

18.3 Staff must regularly review all the systems and processes under their control to ensure they comply with this Data Protection Policy and check that adequate governance controls and resources controls and resources are in place to ensure proper use and protection of personal data.

19. MARKETING AND CONSENT

19.1 The Group will sometimes contact Individuals to send them marketing or to promote the Group. Where the Group carries out any marketing, Data Protection Laws require that this is only done in a legally compliant manner.

19.2 Marketing consists of any advertising or marketing communication that is directed to particular individuals. GDPR has introduced a number of important changes for organisations that market to individuals, including:

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

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

19.3 The Group also needs to be aware of the Privacy and Electronic Communications Regulations (PECR) that sit alongside data protection. PECR apply 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 the Group are not processing any personal data

19.4 Consent is central to electronic marketing. Best practice is to provide an un-ticked opt-in box.

19.5 Alternatively, the Group may be able to market using a “soft opt-in” if the following conditions were met:

19.5.1 contact details have been obtained in the course of a sale (or negotiations for a sale);

19.5.2 the Group are marketing its own similar services; and

19.5.3 the Group 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.

20. AUTOMATED DECISION MAKING AND PROFILING

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

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

Profiling happens where the Group automatically uses Personal Data to evaluate certain things about an Individual.

20.2 Any Automated Decision Making or Profiling which the Group carries out can only be done once the Group is confident that it is complying with Data Protection Laws. If Group

Staff wish to carry out any Automated Decision Making or Profiling they must inform the Data Protection Officer in advance.

20.3 Group Staff must not carry out Automated Decision Making or Profiling without the approval of the Data Protection Officer.

20.4 The Group does not carry out Automated Decision Making or Profiling in relation to its employees.

21. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

21.1 The GDPR requires the Group 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:

21.1.1 describe the collection and use of Personal Data;

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

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

21.1.4 the measures to address the risks.

21.2 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.

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

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

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

21.5.1 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;

21.5.2 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

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

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

22. SHARING PERSONAL DATA

22.1 Generally Personal Data cannot be shared with third parties unless certain safeguards and contractual arrangements have been put in place.

22.2 Group Staff may only share the Personal Data they hold with another employee, agent or representative of our group (which includes our subsidiaries and the ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and transfer complies with any applicable cross-border transfer restrictions.

22.3 Staff may only share the Personal Data they hold with third parties, such as our service providers if:

22.3.1 they have a need to know the information for the purposes of providing the contracted services;

22.3.2 sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

22.3.3 the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

22.3.4 the transfer complies with any applicable cross-border transfer restrictions; and

22.3.5 a fully executed written contract that contains GDPR and approved third-party clauses has been obtained.

23. TRANSFERRING PERSONAL DATA TO A COUNTRY OUTSIDE THE EEA

23.1 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 considered whenever the Group appoints a supplier outside the EEA or the Group appoints a supplier with group companies outside the EEA which may give access to the Personal Data to staff outside the EEA.

23.2 So that the Group can ensure it is compliant with Data Protection Laws, Group Staff must not export Personal Data unless it has been approved by the Data Protection Officer.

23.3 Group Staff must not export any Personal Data outside the EEA without the approval of the Data Protection Officer.

24. CHANGES TO THIS DATA PROTECTION POLICY

24.1 The Group reserves the right to change the Data Protection Policy at any time without notice. The latest copy of this policy will be held on SharePoint.

24.2 This policy was last revised in November 2021. It will be reviewed every three years or earlier if there are any legislative or regulatory changes.

Version	**3**
Date of Issue	**December 2021**
Next Review Date	**December 2024**
Lead	**Vice Principal Finance and Resources**
Approved by	**Executive 07.09.2020; 29.11.21** **Finance and General Purposes Committee 03.12.21**
Published	**College Website, Staff Intranet, Student Intranet**
Equality Impact Analysis	**May 2018**
Equality Analysis Review	**November 2021**
Version 1 - New Policy developed by DPO based on the AoC GDPR compliant template policy developed by Irwin Mitchell Solicitors. Version 2 – Minor updates. Changes to staff titles and policy titles. Version 3 - Minor updates and three year review cycle added.	