reigate•college

Data Protection Policy

June 2021

Review: June 2024

1 Introduction

1.1 Reigate Learning Alliance's ("the Alliance") reputation, stability and growth are dependent on the way we manage and protect Personal Data. Protecting Personal Data and handling it properly and in accordance with Data Protection Laws is a key responsibility of everyone within the Alliance.

1.2 As an organisation that collects, stores and uses Personal Data about its employees, students, alumni, and suppliers, the Alliance recognises that having controls around the collection, storage, use and destruction of Personal Data is important in order to comply with its obligations under Data Protection Laws including under Article 5 of the General Data Protection Regulation (Regulation (EU) 2016/679).

1.3 The Alliance has implemented this Data Protection Policy to ensure all Personnel are aware of what they must do to ensure the correct and lawful treatment of Personal Data.

1.4 Managers are responsible for ensuring that the Personnel they are responsible for (including new starters) are aware of and understand their obligations under this Policy. The Alliance may issue revisions of this Policy from time to time.

1.5 This policy does not form part of any personnel's contract of employment and the Reigate Learning Alliance reserves the right to change this policy at any time. All personnel are obliged to comply with this policy at all times.

1.6 This policy (and the other policies and documents referred to in it) sets out the basis on which the Alliance will collect, store and/or use Personal Data either where the Alliance collects it from Individuals itself, or where it is provided to the Alliance by third parties. It also sets out rules on how personnel must handle Personal Data.

2 Scope

2.1 This Policy applies to all personnel who collect, store and/or use Personal Data and applies to all Personal Data stored electronically, in paper form, or otherwise.

3 Definitions

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

3.1.1 A Controller is responsible for compliance with Data Protection Laws. Examples of Personal Data for which the Alliance is the Controller of include employee, alumni, applicant and student details. Wherever the Alliance decides what Personal Data it is going to collect and store and how it will use it, the Alliance is the Controller of that data.

3.2 Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) as it forms part of domestic law in the United Kingdom by virtue of section 3 of the European Union (Withdrawal) Act 2018 (including as further amended or modified by the laws of the United Kingdom or a part of the United Kingdom from time to time) ("UK GDPR"), the Data Protection Act 2018 and all other applicable laws relating to the collection, storage and use of Personal Data and privacy and any applicable codes of practice issued by the ICO or any other applicable regulator.

3.3 Data Protection Officer – the Alliance's data protection officer from time to time.

3.4 ICO – The Information Commissioner's Office which is the UK's data protection authority that issues guidance and codes of practice about Data Protection Laws and is responsible for enforcing Data Protection Laws in the UK and can impose fines for non-compliance.

3.5 Individuals – Living individuals who can be identified, directly or indirectly, from information that the Alliance 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, alumni, applicants, agents, contractors. Individuals also include partners in partnerships and sole traders.

3.6 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 used in a business-to-business context.

3.6.1 Personal Data is defined very 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.

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

3.8 Processor – A Processor is an Individual or a business, outside the Alliance, engaged by it to perform a service and as part of that service processes (e.g. gets access to or uses) Personal Data on behalf of the Alliance. Examples of Processors include outsourced HR services (Surrey Payroll and Surrey Pensions Services), cloud services and IT and web support providers.

3.9 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.

4 Your general obligations

4.1 You must ensure that you keep confidential all Personal Data that you collect, store, use and come into contact with as part of your role working for the Alliance.

4.2 You must not release or disclose any Personal Data:

- Outside the Alliance
- Inside the Alliance to Personnel not authorised to access the Personal Data

Unless you are doing it in compliance with a written general permission within your department to release the Personal Data or you have specific authorisation from your Departmental Manager or the Data Protection Officer. This includes on phone calls or in emails.

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

5 Data protection principles

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

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary for the purposes for which it is being processed

- 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
- Kept for no longer than is necessary for the purposes for which it is being processed
- 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 sections below.

5.3 In addition to complying with the above requirements the Alliance also has to demonstrate in writing that it complies with them. The Alliance has a number of policies and procedures in place, including this Policy to ensure that the Alliance can demonstrate its compliance. These Policies can be provided in hard copy / or on the Staff Shared Area. Compliance with these additional policies is as important as compliance with this Policy. If you have any questions regarding these policies, please ask the Data Protection Officer.

6 Lawful use of personal data

6.1 In order to collect, store and/or use Personal Data lawfully the Alliance needs to be able to show that it meets one of a number of legal grounds. For ordinary Personal Data, these legal grounds are as follows:

- The individual has given consent to the use of their Personal Data for specific purposes
- The use of the Personal Data is necessary to perform a contract that the individual is a party to or in order to take steps at the request of the individual prior to entering into a contract with them
- The use of the Personal Data is necessary to comply with our legal obligations
- The use of the Personal Data is necessary to protect the individual's vital interests of those of another natural person
- The use of the Personal Data is necessary to perform a task carried out in the public interest
- The use of the Personal Data is necessary for our legitimate interests, except where our interests are overridden by the interests or fundamental rights and freedoms of the individual, in particular where the individual is a child

6.2 In addition when the Alliance collects, stores and/or uses Special Categories of Personal Data, the Alliance has to show that one of a number of additional conditions is met which are:

- The individual has given explicit consent to the use of their Personal Data for specified purposes
- The use of the Personal Data is necessary to carry out our obligations and exercise our specific rights or those of the individual in the field of employment and social security and social protection law
- The use of the Personal Data is necessary to protect the vital interests of the individual or of another natural person where the individual is physically or legally incapable of giving consent

- The use of the Personal Data is carried out in the course of the legitimate activities of a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
- The use relates to Personal Data which are manifestly made public by the individual
- The use of the Personal Data is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- The use of the Personal Data is necessary for reasons of substantial public interest
- The use of the Personal Data is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of an employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- The use of the Personal Data is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices
- The use of the Personal Data is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

6.3 The Alliance will collect, store and/or use Personal Data relating to criminal offences and convictions where this is in accordance with UK Law.

6.4 The Alliance has carefully assessed how it collects, stores and/or uses Personal Data and how it complies with the obligations set out in paragraphs 7.1 and 7.2 and has recorded this on a record of its use of Personal Data. If the Alliance changes how it collects, stores and/or uses Personal Data, the Alliance will need to update this record and may also need to notify individuals about the change. If you therefore intend to change how you collect, store and/or use Personal Data you must notify the Data Protection Officer as soon as possible and in any event within 1 working day who will decide whether the change requires amendments to be made to the record and any other controls which need to apply.

7 Transparent processing – privacy notices

7.1 Where the Alliance collects Personal Data directly from individuals, the Alliance will inform them about how we collect, store and/or use their Personal Data. This is in a privacy notice. The alliance has a number of privacy notices which apply to employees, candidates for employment, students, and alumni. The Alliance's privacy notices are available in hard copy / or on the Staff Shared Area.

7.2 If the Alliance receives Personal Data about an individual from other sources, we will provide the Individual with the relevant privacy notice about how the Alliance will collect, store and/or use their Personal Data (see above). This will be provided as soon as reasonably possible and in any event within one month.

7.3 If the Alliance changes how it collects, stores and/or uses Personal Data, we may need to notify Individuals about the change. If you therefore intend to change how you collect, store and/or use Personal Data you must notify the Data Protection Officer as soon as possible and in any event within 1 working day who will decide whether your intended change requires amendments to be made to the privacy notices and any other controls which need to apply.

8 Data quality

8.1 Data Protection Laws require that the Alliance only collects, stores and/or uses 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 Alliance's record of how it collects, stores and/or uses Personal Data. The Personal Data must also be accurate and kept up to date.

8.2 Accuracy and Relevance of Personal Data

8.2.1 All Personnel that collect and record Personal Data shall ensure that the Personal Data is recorded accurately. They must also keep it up to date and ensure that they limit the Personal Data to that which is adequate, relevant and necessary to meet the purpose for which it is collected, stored and used.

8.3 Obligations where Personal Data is obtained from sources outside the Alliance

8.3.1 All Personnel that obtain Personal Data from sources outside the Alliance shall take reasonable steps to ensure that the Personal Data is recorded accurately, up to date and limited to that which is adequate, relevant and necessary for the purpose for which it is collected, stored and used. This does not require you to independently check the Personal Data obtained. You must, however, ensure that you have contacted the Data Protection Officer to ensure the Personal Data is obtained from a third party who has been approved by the Data Protection Officer and that the legal requirements in the Data Protection Laws have been complied with.

8.4 Ongoing Housekeeping Obligations

8.4.1 In order to maintain the quality of Personal Data, all Personnel that access Personal Data shall ensure that they review, maintain and update it regularly to ensure that it remains accurate, up to date, adequate, relevant and limited to what is necessary for the purpose for which it is collected, stored and used. Please note that this does not apply to Personal Data which the Alliance must keep in its original form e.g. for legal reasons. Examples of what you should think about to appropriately maintain and update Personal Data include:

- Removing out of date records
- Removing duplicate records and merging related records

- Updating records which are not correct

8.5 Requests from Individuals to correct or delete Personal Data

8.5.1 The Alliance recognises the importance of ensuring that Personal Data is amended, rectified, erased or its use restricted where this is appropriate under Data Protection Laws. Any Personnel who receives a request from an Individual for the amendment, rectification, erasure or restriction of the use of their Personal Data must promptly send the request to DPO@reigate.ac.uk for the request to be reviewed and actioned in accordance with Data Protection Laws. Please see section 14 below for further details of how to handle requests that are made by individuals and also the Rights of Individuals Procedure which works in conjunction with this Policy. This Policy is provided in hard copy / or on the Staff Shared Area.

9 Retention of personal data

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

9.2 The Alliance has assessed, by department and function within the Alliance, the types of Personal Data that it collects, stores and/or uses and the purposes it uses it for. The retention periods that the Alliance has set for the different Personal Data streams within the Alliance are set out on the record of how the Alliance uses Personal Data which is available in hard copy/or on the Staff Shared Area. Please familiarise yourself with how long you may keep Personal Data.

9.3 The deletion of Personal Data will be done securely in accordance with good industry practice that makes it unreadable and unrecoverable. This is the case in relation to both the shredding of physical documents and the wiping of electronic media.

9.4 If you feel that a particular piece of Personal Data needs to be kept for more or less time than the retention periods referred to above, or if you have any questions about this Policy or how long the Alliance keeps Personal Data for, you should contact the Data Protection Officer for guidance.

10 Data security

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

10.2 You must comply with the Alliance's security procedures in relation to information security and the security of Personal Data. Details of these can be obtained from the Data Protection Officer.

10.3 The Alliance also takes the recovery of information very seriously and in the event of a security failure or data breach (see paragraph 12 below) you should follow the instructions of the Data Protection Officer.

11 Data breach

11.1 Whilst the Alliance 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.

11.2 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 something done by a third party, they can also happen as a result of something Personnel within the Alliance do.

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

- Confidentiality breach – this is where there is an unauthorised or accidental disclosure of, or access to, Personal Data e.g. hacking, accessing internal systems that Personnel are not authorised to access, accessing Personal Data stored on a lost laptop, phone or other device, people outside the Alliance gaining access to Personal Data they have no right to access, putting the wrong letter in the wrong envelope, sending an email to the wrong person, or disclosing information over the telephone to the wrong person.
- Availability breach – this is 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 where there is no back up or where the encryption key is lost, 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.
- Integrity breach – where there is an unauthorised or accidental alteration of Personal Data.

11.4 You must notify any potential Personal Data breach to the Data Protection Officer, no matter how big or small and whether or not you think a breach has occurred or is likely to occur using the Personal Data Breach Notification Form which is available in hard copy / or on the Staff Shared Area.

11.5 You may be notified by a third party e.g. a supplier that we outsource services to that they have had a breach that affects Alliance's Personal Data. You must notify the Data Protection Officer by email at DPO@reigate.ac.uk immediately after being notified by a third party.

11.6 If the Personal Data breach involves the loss of a laptop, phone or other mobile device, please immediately notify it to the Data Protection Officer using the Personal Data Breach Notification Form.

11.7 Any notification to the Data Protection Officer under this section of the Policy must be done immediately and always within 24 hours, even if outside of working hours.

11.8 A Personal Data breach will be managed by the Data Protection Officer who will consider whether to seek external legal advice. Personnel may be asked to assist the Data Protection Officer in investigating the Personal Data breach and shall provide all co-operation and information required by the Data Protection Officer.

11.9 Under Data Protection Laws, the Alliance may have to notify the Regulator and also possibly the individuals affected about the Personal Data breach. Notification of a Personal Data breach must be made to the Regulator without undue delay and where feasible within 72 hours of when the Alliance becomes aware of the breach. It is therefore imperative that you notify all Personal Data breaches to Data Protection Officer immediately and always within 24 hours. You must not notify a Personal Data breach to the Regulator or to any Individual affected by yourself. Any notification will be done by or with the authority of the Data Protection Officer.

11.10 All Personal Data breaches or potential Personal Data breaches will be recorded on an Internal Personal Data Breach Register maintained by the Data Protection Officer.

12 Appointing contractors, third parties or service providers who access the Alliance's personal data

12.1 If the Alliance appoints an Individual or a business, outside the Alliance, to perform a service and as part of that service they get access to or use Personal Data on behalf of the Alliance they will be a Processor of the Alliance's Personal Data. Data Protection Laws require that the Alliance only appoints them where the Alliance has carried out sufficient due diligence and has appropriate contracts in place.

12.2 The Data Protection Officer will determine what due diligence must be done on a case-by-case basis. If you propose to appoint an Individual or a business, outside the Alliance, as a Processor of the Alliance's Personal Data you must immediately contact the Data Protection Officer before they are appointed and follow their instruction as to what due diligence must be done. If you are uncertain about whether the Individual or business you are contracting with will be a Processor you must ask the Data Protection Officer before proceeding.

12.3 In addition to carrying out appropriate due diligence, a Processor must be appointed on the basis of a written contract which contains sufficient guarantees to the Alliance to ensure that the Personal Data is kept

confidential and secure and is handled in a way which meets the obligations under Data Protection Laws. All contracts and terms and conditions with Processors must therefore be approved by the Data Protection Officer before acceptance. The service must not begin until the contract or terms and conditions have been approved by the Data Protection Officer.

12.4 The Alliance will monitor the Processor's ongoing compliance with the protections and guarantees given to the Alliance in accordance with Data Protection Laws. You must therefore follow the Data Protection Officer's directions in relation to this.

12.5 The Alliance may share Personal Data with another company who would be considered a Controller where they have control over how they will use the Personal Data. If you intend to share the Alliance's Personal Data with an Individual or business who may be a Controller, you must immediately notify the Data Protection Officer and follow their direction in advance of sharing the Personal Data.

12.6 The Alliance has put in place arrangements to deal with the sharing of Personal Data within the Alliance.

13 Individuals' rights

13.1 The Alliance will collect, store and/or use all Personal Data in accordance with the rights given to individuals' under Data Protection Laws, in particular their rights to:

- Request access to any Personal Data the Alliance holds about them
- Have any inaccurate Personal Data the Alliance hold about them corrected
- Have Personal Data erased in certain circumstances
- Have the use of their Personal Data restricted, including preventing the use of their Personal Data for direct marketing purposes
- Object to processing, including objecting to direct marketing or querying whether the Alliance has a legitimate interest
- Have their Personal Data provided to them, in certain circumstances, in an electronic, commonly used format; and
- Withdraw consent to the use of their Personal Data

13.2 If an individual makes a request to exercise any of these rights, you must contact the Data Protection Officer immediately at DPO@reigate.ac.uk. The Data Protection Office will deal with the request in compliance with data protection law.

13.3 The Alliance will ensure that it allows individuals to exercise their rights in accordance with Data Protection Laws. You must contact the Data Protection Officer if you receive a request from an Individual to exercise any

of the rights set out above. You must follow the instruction of the Data Protection Officer in relation to the handling of these requests.

14 Marketing and consent

14.1 Under Data Protection Laws, marketing has a broad definition which extends to all promotional communications and unsolicited communications (for example emails regarding new courses developments to students).

14.2 The Alliance will sometimes contact individuals to send them marketing or to promote the Alliance and its products and services. Data Protection Laws regulate the use of Personal Data for marketing to individuals, sole traders, partnerships and individuals within companies. The Alliance carries out marketing in accordance with Data Protection Laws based on prospective students' consent and preferences around marketing using the method of contact provided.

14.3 Under Data Protection Laws, for consent to be valid it must meet strict requirements. Consent to marketing is therefore taken centrally by the Alliance. You must not send or knowingly allow marketing to be sent to individuals who have not provided marketing consent. If for any reason you feel that consent is not appropriate in a particular situation, you must contact the Data Protection Officer and get their authorisation before sending marketing without consent.

14.4 When an individual has given consent to send them marketing, this consent will be valid for 2 years from the date they have given it. The Alliance will therefore contact individuals who have given consent to send them marketing before the expiry of the 2 years to ensure they are still happy for the Alliance to contact them for marketing purposes.

14.5 The individual will have the right under Data Protection Laws to withdraw their consent at any time or the change their preferences. If an Individual withdraws their consent the Alliance will no longer be able to market to them.

14.6 You should be aware that failure to comply with Data Protection Laws in relation to marketing is often the subject of fines or sanctions by the ICO. You must therefore consult with our Data Protection Officer if you have any questions or concerns about marketing.

15 Automated decision-making and profiling

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

15.1.1 Automated Decision Making happens where the Alliance makes a decision about an Individual solely by automated means (without any human involvement) and the decision has legal or other significant effects.

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

15.2 The Alliance does not currently carry out Automated Decision Making in relation to individuals in the EEA or the UK, nor does it carry out profiling in relation to tailoring marketing.

15.3 Before any Automated Decision Making or Profiling is carried out by the Alliance a risk assessment must be done as to whether this activity is in accordance with Data Protection Laws. This is done via a Data Protection Impact Assessment (DPIA) which is considered below.

15.4 You must not carry out Automated Decision Making or Profiling in addition to that set out in our privacy notices without the approval of the Data Protection Officer.

16 Data Protection Impact Assessments (DPIA)

16.1 Where the Alliance is launching or proposing to adopt a new process, product or service which involves Personal Data, the Alliance needs to consider whether it needs to carry out a risk impact assessment to ensure that its collection, storage and/or use of Personal Data is proportionate and in accordance with Data Protection Laws. This impact assessment is called a Data Protection Impact Assessment or DPIA. The Alliance needs to carry out a DPIA at an early stage in the process so that the Alliance can identify and remedy 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.

16.2 Examples of where a DPIA should be carried out include the following (please note that this list is not exhaustive):

- Installing new CCTV cameras/system
- Profiling of customers
- Monitoring or profiling of staff
- Automated decision making
- Additional uses of health data or Personal Data relating to criminal convictions and offences

16.3 You must therefore notify the Data Protection Officer of all new processes, products or services which you propose to adopt or to buy from third parties which involve Personal Data. You must not begin using Personal Data in any new process, project or service without obtaining approval by the Data Protection Officer. You must co-operate with and complete all documentation required by the Data Protection Officer.

17 Transferring personal data to a country outside the UK

17.1 Data Protection Laws impose strict controls on Personal Data being transferred to other entities and individuals who are based outside the UK. If, therefore, you intend to transfer Personal Data in this way you must notify the Data Protection Officer before it is done and follow their direction so as to ensure that the export is compliant with Data Protection Laws.

18 Consequences of breaching this policy

18.1 Breach of this Policy, concealing breaches or concealing or falsifying related facts may result in sanctions or disciplinary action taken against Personnel. This may include termination of employment. In some cases, the Alliance may report breaches to law enforcement authorities. Any Personnel who are aware of a breach of this Policy must contact the Data Protection Officer as soon as possible (see above for contact details).

19 Retention of data

19.1 The Alliance will retain categories of data for different lengths of time but, due to the limitation on storage space, data cannot be kept indefinitely, unless there are specific requests to do so. In general, data will be retained for the following maximum periods of time:

Data subject	**Duration**
Employees/workers	6 years
Students	6 years
Others	6 years