ALTUS
EDUCATION PARTNERSHIP

Altus Education Partnership

General Data Protection Policy

Approval Body	**Trust Board**
Date of Approval	**18/12/2019**

1. Overview

Altus Education Partnership (the trust) recognises that the reputation and future growth of the trust are dependent on the way the trust manages and protects personal data. Protecting the confidentiality and integrity of personal data is a key responsibility of everyone within the trust.

As an organisation that collects, uses and stores personal data about its employees, suppliers (sole traders, partnerships or individuals within companies), applicants (student and staff applications), students, trustees and local academy council members, parents and visitors, the trust recognises that having controls around the collection, use, retention and destruction of personal data is important in order to comply with the trust's obligations under data protection laws and in particular its obligations under Article 5 of GDPR.

The trust 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. This will maintain confidence in the trust and will provide for a successful working and learning environment for all.

All trust personnel will receive training on the new general data protection regulations to ensure that all personnel are aware of their obligations under the GDPR.

Personnel employed by the trust will receive a copy of this policy when they start and may be notified of periodic revisions of this policy accessed through the VLE. This policy does not form part of any personnel's contract of employment and the trust reserves the right to change this policy at any time. All trust personnel are obliged to comply with this policy at all times.

Any queries concerning this policy should be directed to the Data Protection Officer, who is responsible for ensuring the trust'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 trust will collect and use personal data either where the trust collects it from individuals itself, or where it is provided to the trust by third parties. It also sets out rules on how the trust handles uses, transfers and stores personal data.

It applies to all personal data stored electronically, in paper form, or otherwise.

3. Definitions

3.1. **Trust** – the trust board of the Altus Education Partnership
3.2. **College** – Rochdale Sixth Form College
3.3. **Trust Personnel** – Any trust employee, worker or contractor who accesses any of the trust's personal data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the trust.
3.4. **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 controller is responsible for compliance with data protection laws. Examples of personal data the trust is the controller of include employee details or information the trust collects relating to students. The trust will be viewed as a controller of personal data if it decides what personal data the trust is going to collect and how the data will be used.

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.

3.5. **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 –** The Data Protection Officer is Kirk Charlesworth-Cairns, who can be contacted at: 01706 769 800, k.charleswoth-cairns@rochdalesfc.ac.uk.

3.7. **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 the trust has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if this information can be used to work out who they are. Individuals include employees, students, parents, visitors and potential students. Individuals also include 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.

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. Trust Personnel's General Obligations

4.1. All trust personnel must comply with this policy.

4.2. Trust 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. Trust personnel must not release or disclose any personal data:

4.3.1. outside the trust; or

4.3.2. inside the trust to trust 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. Trust personnel must take all steps to ensure there is no unauthorised access to personal data whether by other trust personnel who are not authorised to see such personal data or by people outside the trust.

5. Data protection principles

5.1. When using personal data, data protection laws require that the trust 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 the trust also has to demonstrate in writing that it complies with them. The trust has a number of policies and procedures in place, including this policy and the documentation referred to in it, to ensure that the trust can demonstrate its compliance.

6. Lawful use of personal data

6.1. In order to collect and/or use personal data lawfully the trust needs to be able to show that its use meets one of a number of legal grounds. The legal grounds for processing personal data can be found on the website of the Information Commisioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing

6.2. In addition when the trust collects and/or uses special categories of personal data, the trust has to show that one of a number of additional conditions is met. The additional conditions can also be found on the website of the Information Commisioner's Office: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/special-category-data.

6.3. The trust 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 the trust changes how it uses personal data, this record must be updated and the trust may also need to notify Individuals about the change. If trust personnel therefore intend to change how they use personal data at any point they must notify the Data Protection Officer who will decide whether their intended use requires amendments to be made and any other controls which need to apply.

7. Transparent processing – privacy notices

7.1. Where the trust collects personal data directly from Individuals, the trust will inform them about how personal data will be used. This is in a privacy notice.

7.2. If the trust receives personal data about an Individual from other sources, the trust will provide the Individual with a privacy notice about how their personal data will be used. This will be provided as soon as reasonably possible and in any event within one month.

7.3. If the trust changes how it uses personal data, the trust may need to notify Individuals about the change. If trust personnel therefore intend to change how they use personal data, the Data Protection Officer should be notified in order for a decision to be made on whether the trust personnel's intended use requires amendments to be made to the privacy notices and any other controls which need to apply.

8. Data quality – ensuring the use of accurate, up to date and relevant personal data

8.1. Data protection laws require that the trust 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 **Error! Reference source not found.** above) and as set out in the trust's record of how it uses personal data. The trust is also required to ensure that the personal data the trust holds is accurate and kept up to date.

8.2. As part of the preparation for GDPR, the trust has carried out an information asset audit and this forms a key part of the GDPR documentation. The information asset audit will be updated whenever there is a change to the way personal data is collected or used and in any event, annually.

8.3. All trust personnel that collect and record personal data shall ensure that the 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.

8.4. All trust personnel that obtain personal data from sources outside the trust 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 trust personnel to independently check the personal data obtained.

8.5. In order to maintain the quality of personal data, all trust 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 the trust must keep in its original form (e.g. for legal reasons or that which is relevant to an investigation).

8.6. The trust 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 trust has a Rights of Individuals Policy and a Rights of Individuals Procedure which set out how the trust 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 the trust does not keep personal data longer than is necessary for the purpose or purposes for which the trust collected it.

9.2. The trust 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 trust, the reasons for those retention periods and how the trust securely

deletes personal data at the end of those periods. These are set out in the Data Retention Policy.

9.3. If trust 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 trust personnel have any questions about this policy or the trust's Personal data retention practices, they should contact the Data Protection Officer for guidance.

10. Data Security

The trust 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. The trust 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 the trust 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 trust personnel must comply with the trust's data breach notification policy. See paragraphs 11.2 and 11.3 for examples of what can be a personal data breach. All trust personnel must familiarise themselves with it as it contains important obligations which trust personnel need to comply with in the event of personal data breaches.

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 action taken by a third party, they can also occur as a result of something someone internal does.

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 member of trust 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 ransom ware, deleting personal data in error, loss of access to personal data stored on

systems, inability to restore access to personal data from back up, or loss of an encryption key; and

11.3.3. **Integrity breach** - where there is an unauthorised or accidental alteration of personal data.

12. Appointing contractors who access the trust's personal data

12.1. If the trust appoints a contractor who is a processor of the trust's personal data, data protection laws require that the trust only appoints them where the trust has carried out sufficient due diligence and only where the trust has appropriate contracts in place.

12.2. 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.

12.3. Any contract where an organisation appoints a processor must be in writing.

12.4. GDPR requires the contract with a processor to contain the following obligations as a minimum:

12.4.1. to only act on the written instructions of the controller;

12.4.2. to not export personal data without the controller's instruction;

12.4.3. to ensure staff are subject to confidentiality obligations;

12.4.4. to take appropriate security measures;

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

12.4.6. to keep the personal data secure and assist the controller to do so;

12.4.7. to assist with the notification of data breaches and data protection impact assessments;

12.4.8. to assist with subject access/individuals rights;

12.4.9. to delete/return all personal data as requested at the end of the contract;

12.4.10. to submit to audits and provide information about the processing; and

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

12.5. In addition the contract should set out:

12.5.1. The subject-matter and duration of the processing;

12.5.2. the nature and purpose of the processing;

12.5.3. the type of personal data and categories of individuals; and

12.5.4. the obligations and rights of the controller.

13. Individual's rights

13.1. 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.

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

13.3. **Subject Access Requests**

13.3.1. Individuals have the right under the GDPR to ask the trust 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 has been reduced from 40 days to one month (with a possible extension if it is a complex request). The trust is not able to charge a fee for complying with the request.

13.3.2. 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.

13.4. **Right of Erasure (Right to be Forgotten)**

13.4.1. This is a limited right for individuals to request the erasure of personal data concerning them where:

13.4.1.1. the use of the personal data is no longer necessary;

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

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

13.4.1.4. the personal data has been unlawfully processed; and

13.4.1.5. the personal data has to be erased for compliance with a legal obligation.

13.4.2. 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.

13.5. **Right of Data Portability**

13.5.1. 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

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

13.6. **The Right of Rectification and Restriction**

13.6.1. 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.

13.7. The trust 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 trust's Rights of Individuals Policy and Rights of Individuals Procedure.

14. Marketing and consent

14.1. Marketing consists of any advertising or marketing communication that is directed to particular individuals.

14.2. The trust does not currently contact Individuals to send them marketing or to promote the trust or Rochdale Sixth Form College.

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.

Automated decision making happens where the trust 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 trust automatically uses personal data to evaluate certain things about an Individual.

15.2. Any automated decision making or profiling which the trust carries out can only be done once the trust is confident that it is complying with data protection laws. If trust personnel therefore wish to carry out any automated decision making or profiling trust personnel must inform the Data Protection Officer.

15.3. Trust personnel must not carry out automated decision making or profiling without the approval of the Data Protection Officer.

15.4. The trust does not currently use personal data for profiling or automated decision making, for students or trust personnel.

16. Data protection impact assessments (DPIA)

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

16.1.1. describe the collection and use of personal data;

16.1.2. assess its necessity and its proportionality in relation to the purposes;

16.1.3. assess the risks to the rights and freedoms of individuals; and

16.1.4. the measures to address the risks.

16.2. 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.

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

16.4. Where the trust is launching or proposing to adopt a new process, product or service which involves personal data, the trust needs to consider whether it needs to carry out a DPIA as part of the project initiation process. The trust needs to carry out a DPIA at an early stage in the process so that any problems with the new process, product or service can be identified and fixed at an early stage, reducing the associated costs and damage to reputation, which might otherwise occur.

16.5. Situations where the trust may have to carry out a data protection impact assessment include the following (this list is not exhaustive):

16.5.1. 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;

16.5.2. 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

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

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

17. Transferring personal data to a country outside the EEA

17.1. 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. The information asset audit carried out has not identified any processors or suppliers currently in use outside the EEA. This policy will be updated should this change.

17.2. So that the trust can ensure it is compliant with data protection laws trust personnel must not export personal data outside the EEA unless it has been approved by the Data Protection Officer.