GENERAL DATA PROTECTION REGULATIONS POLICY

AUTHOR: **Human Resources**

DATE: **July 2020**

Version **3**

GENERAL DATA PROTECTION REGULATIONS POLICY

1 PURPOSE

The objective of this policy is to ensure that:

- all members of staff (authorised data processors) are familiar with their obligations under the General Data Protections Regulations (GDPR) 2018.
- all data processing carried out by the College complies with the GDPR and is in line with the six data protection principles and the registered purpose groups.

This policy also sets out the procedures and fees for data subject access requests regarding general data and CCTV access requests.

2 SCOPE

This policy applies to:

- all employees at Calderdale College
- all external projects managed by Calderdale College's External Funding Unit, including European Social Funded training programmes. Please refer to Appendix J for the GDPR requirements specific to the current European Social Funded training programmes.

Responsibilities under GDPR:

- **Data Controller** (The College) - determines the purposes and means of processing personal data. A controller is not relieved of their obligations where a processor is involved – the GDPR places further obligations on the controller to ensure contracts with processors comply with the GDPR.

- **Data Protection Officer (DPO)** (Clerk to the Governors) - informs and advises the College and its employees about their obligations to comply with the GDPR and other data protection laws. They monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits, they are the first point of contact for supervisory authorities and for individuals whose data is processed (employees, customers etc…)

- **Data Processor** (All staff) – are responsible for processing personal data on behalf of a controller. If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. Processors will have legal liability if they are responsible for a breach. All Calderdale College employees are Data Processors and should be aware of their responsibilities under the GDPR, this policy and process data lawfully. To ensure that

all data is kept protected and secure i.e. information is not disclosed without authority, information is not left unattended on photocopiers, pcs are secured with a password etc…

- **Senior Leadership Team (SLT) and College Management Team (CMT):** To ensure that Data Processors and agents within their own area are fully aware of their obligations under the GDPR 2018 and this policy to ensure compliance with the law. Furthermore, failure to prevent unauthorised users from accessing personal data may lead to legal sanctions (personal and corporate) under the GDPR.

Compliance with this Policy and Codes of Practice will be subject to internal and external audit.

Failure to comply with the GDPR 2018 and/or this policy could result in:

- legal and/or disciplinary proceedings being instigated against any member of staff or agent.
- personal as well as corporate liability.
- Fees – please see section 8

Any member of staff, who considers that the policy has not been followed in respect of personal data about themselves, should raise the matter with the designated Data Protection Officer initially. If the matter is not resolved it should be raised as a formal grievance.

Potential impact on Equality, Diversity and Inclusion

All staff will ensure that procedures and processes are carried out to minimise barriers to all protected characteristics and that reasonable adjustments are made to allow opportunity for all.

3 DETAILS OF POLICY

3.1 Data Protection Principles

The College needs to keep certain information about its employees, students and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with. To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, the College must comply with the General Data Protection Regulations, which gives people specific rights in relation to their personal information and also place certain obligations on organisations that are responsible for processing personal data.

The GDPR applies to 'personal and sensitive personal data':

- **Personal data** means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

- **Sensitive Personal data** refers to special categories of personal data such as race, religion, genetics, biometrics or sexual orientation etc.…Staff and learners will be asked for express consent for the College to process sensitive personal data.

GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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."

It requires that the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this General Data Protection Regulations Policy.

3.2 There are six lawful bases for processing

At least one of these must apply whenever personal data is processed:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's

personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

3.3 The Purpose Groups and Notification of Data Processed and Held

Calderdale College is registered with the Information Commissioner on the register of Data Controllers for the processing of data held within eight purpose groups.

In order for the College to process lawfully under the GDPR all data processors must understand what data can be processed by their department.

It is therefore a requirement that all persons responsible for processing personal data are fully aware of the purpose groups with which the College is registered to process data. It is not reasonable to expect that anyone unfamiliar with the purpose groups would be able to assist the College in its obligations to comply with the act and consequently the law.

The purpose groups are:

1. Staff, Agent and Contractor Administration
2. Advertising, Marketing, Public Relations, General Advice Services
3. Accounts and Records
4. Education
5. Learner and Staff Support Services
6. Crime Prevention and Prosecution of Offenders
7. Method 2: Data Controllers Further Description of Purpose: Provision of Facilities to Other Groups or Organisation
8. Method 2: Data Controllers Further Description of Purpose: Publication of the College Magazine

If the purpose groups above do not cover data you are processing, or envisage will require to process, you must advise the Data Protection Officer immediately. Additional purpose groups can be requested to be included on the College Data Protection Registration from the ICO. The Data Protection Officer must administer this process in all case.

Note The above Purpose groups are summarised versions from the registration. The full purpose group descriptions are available from the Data Protection Officer.

3.4 The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

3.4.1 The right to be informed

The right to be informed encompasses the Colleges obligation to provide ‘fair processing information’, typically through a privacy notice.

The information the College supplies about the processing of personal data must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

The table below summarises the information the College should supply to individuals and at what stage.

What information must be supplied?	**Data obtained directly from data subject**	**Data not obtained directly from data subject**
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data		✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each of data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from and whether it came from publicly accessible sources		✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓
When should information be provided?	At the time the data are obtained	Within a reasonable period of having obtained the data (within one month) If the data are used to communicate with the individual, at the latest, when the first

		communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.

3.4.2 The right of access

Under the GDPR, individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice.

This allows employees to access their personal data so that the individual is aware of and can verify the lawfulness of the processing of that data.

The College will provide a copy of the information **free of charge**. However, it can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

We may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that we can charge you for all subsequent access requests.

The fee will be based on the administrative cost of providing the information.

How long does the College have to comply?

Information must be provided without delay and at the latest within one month of receipt.

The College is able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, the College will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

How will the information be provided?

The College will verify the identity of the person making the request, using 'reasonable means' and if the request is made electronically, we will provide the information in a commonly used electronic format.

What about requests for large amounts of personal data?

Where the College processes a large quantity of information about an individual, the GDPR permits the College to ask the individual to specify the information the request relates to.

The GDPR does not include an exemption for requests that relate to large amounts of data, but the College may be able to consider whether the request is manifestly unfounded or excessive.

3.4.3 The right to rectification

Individuals have the right to have personal data rectified if it is inaccurate or incomplete.

If the College has disclosed the personal data in question to others, we would contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, the College would also inform the individual which this affects about these recipients.

How long does the College have to comply with a request for rectification?

The College must respond within one month.

This can be extended by two months where the request for rectification is complex.

Where the College is not taking action in response to a request for rectification we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy.

3.4.4 The right to erasure

Individuals have the right to have personal data erased and to prevent processing in certain circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (ie otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

The College can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- for public health purposes in the public interest;
- archiving purposes in the public interest, scientific research historical research or statistical purposes; or
- the exercise or defence of legal claims.

Will the College tell other organisations about the erasure of personal data?

If the College has disclosed the personal data in question to others, we will contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we will also inform the individuals about these recipients.

The GDPR reinforces the right to erasure by clarifying that organisations in the online environment who make personal data public should inform other organisations who process the personal data to erase links to, copies or replication of the personal data in question.

3.4.5 The right to restrict processing

Individuals have a right to block or suppress processing of personal data in the following circumstances

- Where an individual contests the accuracy of the personal data, you should restrict the processing until you have verified the accuracy of the personal data.

- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and you are considering whether your organisation's legitimate grounds override those of the individual.

- When processing is unlawful and the individual opposes erasure and requests restriction instead.

- If you no longer need the personal data but the individual requires the data to establish, exercise or defend a legal claim.

The College is permitted to store the personal data of the individual, but not further process it.

3.4.6 The right to data portability

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

The College will comply by:

- Providing the personal data in a structured, commonly used and machine readable form. Open formats include CSV files. Machine readable means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.
- The information will be provided free of charge.
- If the individual requests it, the College may be required to transmit the data directly to another organisation if this is technically feasible. However, the College is not required to adopt or maintain processing systems that are technically compatible with other organisations.
- If the personal data concerns more than one individual, the College will consider whether providing the information would prejudice the rights of any other individual.

How long does the College have to comply?

We will respond without undue delay, and within one month. This can be extended by two months where the request is complex or we receive a number of requests. We will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where the College is not taking action in response to a request, we will explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

3.4.7 The right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

How does the College comply with the right to object if it processes personal data for the performance of a legal task or the College's legitimate interests?

Individuals must have an objection on "grounds relating to his or her particular situation".

The College must stop processing the personal data unless:

- it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

The College must inform individuals of their right to object "at the point of first communication" and in the Colleges privacy notice.

How does the College comply with the right to object if it processes personal data for direct marketing purposes?

The College must stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse.

The College will deal with an objection to processing for direct marketing at any time and free of charge.

We will inform individuals of their right to object "at the point of first communication" and in our privacy notice.

This must be "explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information".

How does the College comply with the right to object if it processes personal data for research purposes?

Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

If the College conducts research where the processing of personal data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

3.4.8 Rights in relation to automated decision making and profiling

The GDPR has provisions on:

- automated individual decision-making (making a decision solely by automated means without any human involvement); and
- profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.

The College can only carry out this type of decision-making where the decision is:

- necessary for the entry into or performance of a contract; or
- authorised by Union or Member state law applicable to the controller; or
- based on the individual's explicit consent.

3.5 Accountability and Governance

Whenever a controller uses a processor, (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place.

Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR, and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase data subjects' confidence in the handling of their personal data.

3.6 Documentation?

The College must document the following information:

- The name and contact details of the College (and where applicable, of other controllers, your representative and your Data Protection Officer).
- The purposes of the processing.
- A description of the categories of individuals and categories of personal data.
- The categories of recipients of personal data.
- Details of any transfers to third countries including documenting the transfer mechanism safeguards in place.
- Retention schedules.
- A description of the College's technical and organisational security measures.

3.7 Data Guide

To ensure compliance with the GDPR 2018 Calderdale College has established a Data Guide system. Familiarity and understanding of the Data Guide will ensure that all College data processors and agents of the College contribute effectively in complying with this policy and the General Data Protection Regulations.

3.8 Personal Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

When a security incident takes place, the College will quickly establish whether a personal data breach has occurred and, if so, promptly take steps to address it, including telling the ICO if required.

When a personal data breach has occurred, the College will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is likely that there will be a risk then we will notify the ICO; if it is unlikely then the College doesn't have to report it.

If a College data processor (third party) suffers a breach, then that processor must inform the College without undue delay as soon as it becomes aware. The College will in turn notify the ICO.

The College has to report a notifiable breach to the ICO without undue delay, but not later than 72 hours after becoming aware of it. If the College takes longer than this, then reasons for the delay will be given.

When reporting a breach, the College must provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
  the name and contact details of the data protection officer or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Controllers will prioritise the investigation, give it adequate resources, and expedite it urgently. We must notify the ICO of the breach when we become aware of it, and submit

further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.

When do we need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, the GDPR says you must inform those concerned directly and without undue delay. In other words, this should take place as soon as possible.

A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO. Again, you will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, you will need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

What information must we provide to individuals when telling them about a breach?

You need to describe, in clear and plain language, the nature of the personal data breach and, at least:

- the name and contact details of your Data Protection Officer (if your organisation has one) or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

3.9 Enforcement Action

Violations of the following can result in a significant fine up to 10 million euros or 2% of the College's turnover:

- internal record keeping
- data processor contracts
- data security
- breach notifications
- data protection officers
- data protection by design or default

Violations of the follow can result in a significant fine up to 20 million euros or 4% of the College's turnover:

- breaches of data protection principles
- conditions for consent
- data subjects rights and
- international data transfers

3.10 Children

Children aged 13 or over are able provide their own consent in relation to data protection. You may therefore need to verify that anyone giving their own consent in these circumstances is old enough to do so. Children under this age you need to get consent from whoever holds parental responsibility for them - unless the ISS you offer is an online preventive or counselling service.

3.11 Security of Personal Data

Data processors must ensure that personal data (and sensitive data for those authorised to process sensitive data) are stored securely. Data may be stored in either hard files or electronically. The storage system used in either case will be classified under the GDPR as a "Relevant Storage System" if it is possible to locate personal data through an indexing or similarly organised systematic process to enable the retrieval of personal or sensitive.

Computers which are used to store personal data (and sensitive data for those authorised to process sensitive data) must be password protected and have installed automatic timed out locking facilities. Personal PCs and any other mobile devices are the responsibility of the user and all efforts to ensure that these devices are safe at all times must be made. Please refer to Appendix A for help and advice on security.

Where personal data (and sensitive data for those authorised to process sensitive data) is stored on a data stick, or any other form of storage device, that must be issued by the College IT Department which is encrypted and password protected. Mobile data storage devices are the responsibility of the user and all efforts to ensure that these devices are safe at all times must be made. Please refer to Appendix A for help and advice on security.

Where personal data is stored on a shared drive or local group, the data processor/s must ensure that only authorised data processors within that particular purpose group have access to the data. This includes physical access to the PC/Device onto which that data is stored or being used and also from the viability of non-data processors by way of viewing the screen on to which the data is displayed.

In situations where all personnel in a particular shared drive or local group are not authorised data processors for the relevant purpose group, the authorised data processor/s must ensure that access to that data are only available to the authorised data processors for the purpose group. This may necessitate that the data are stored in personal electronic files protected from unauthorised access.

Where hard copy files are used to store personal data (or sensitive data for those authorised to process sensitive data) they should be locked when not in use in a secure cabinet or, when in use, in an office which is staffed/supervised at all times by authorised data processors and that is locked shut when not staffed.

Personal data must not be stored in an environment that is not secure or would allow access by unauthorised parties, this includes data processors not authorised for a particular purpose group.

Data must be stored in an environment, which ensures that the data are protected from the risk of accidental loss or damage. Where loss or damage to data would affect the operation of the College or specific department then this should be noted on the College or departmental risk register accordingly.

Where it is necessary to print personal or sensitive data please ensure that only Data Controllers are able to access the printed material. Do not send data to orbital printers where it cannot be immediately retrieved by the person printing/requiring that data.

Your attention is also drawn to the advice provided at appendix A of this policy.

3.12 Data Subject Access Procedures

All persons who are the subject of personal data have a right to request and view personal and sensitive data stored about them. Such a request under the GDPR is referred to as a "Data Subject Access Request".

All data subject access requests (Appendix C & D) must be immediately forwarded to the Data Protection Officer. The Data Protection Officer will, in each case, make an assessment of the validity of the data subject access request. All requests will be formally registered by the Data Protection Officer along with all consequent actions pertaining to each request.

The College has one month (from the first full day following the request) to formally respond to any data subject access request. There is the possibility to extend this period for particularly complex requests.

In the case of a CCTV data subject access request (Appendix D) the Data Protection Officer will pass the data subject request to the Senior Facilities Manager or Security Supervisor who will administer the CCTV subject access procedure.

All data subject access requests will be logged onto a single data subject access log which will be administered only by the Data Protection Officer. The Data Protection Officer will forward to the applicant a fee request notice (where applicable – when a request is manifestly unfounded or excessive) once in receipt of the subject access request forms. Fee notice request is attached as Appendix E.

The data processor receiving the data subject access request should date stamp the access request letter before forwarding to the Data Protection Officer.

In the event of a data processor receiving a verbal request for data subject access the data processor should advise the applicant that the request must be in writing and addressed to the Data Protection Officer.

The Data Protection Officer will administer the data subject access request process. It may be necessary to involve other data processors in the administration of the subject access request.

Where a subject access request involves other data processors, sufficient time and resource must be made available by the relevant SLT and CMT member to ensure that the College meets the deadline obligations set out in the GDPR (one month).

The Data Protection Officer will maintain and update as necessary the data subject access log of the data subject access request process in each specific case.

In any subject access request the official data subject access request forms must be used. These are included to this policy as appendices C and D.

3.13 College Data Retention

All College records, whether they contain personal, sensitive or any other type of information not covered by the GDPR will be kept in accordance with the QAP 4.02 Control, Storage & Retention of College Records Procedure.

Each department within the College is responsible for ensuring that all records for retention are correctly and securely boxed up in appropriate and approved archive storage boxes. All boxes must be marked externally with the details of the contents, the identification of the department to which they relate and the disposal date.

Archive boxes are a standard size and are flat pack. The Archive Box Request Form should be completed and send to the Estates & Facilities Office. Once the form has been authorised, boxes will be issues with a reference number for tracking purposes. The end of each box should be marked with any identifying information that you require and a log created against the reference number for retrieval purposes. It is critical that the date for destruction is accurate stating the month and year.

As the boxes should only contain paper and/or cardboard, it is important that plastic pockets, ring binders, lever arch files etc. must not be placed in the boxes. As a solution, rubber bands and bankers envelopes can be used to keep documents together. This ensures that both the cost of secure waste disposal is as low as possible and it reduces the number of boxes that will require off-site storage.

Once boxes are ready for collection, please contact the Estates and Facilities helpdesk and the location of storage will be decided based upon the available space. At least one week should be allowed from an initial request to remove the boxes as transport will require booking.

Whilst boxes can be retrieved from storage within forty eight hours of a request, there is a response and delivery charge where the size of the charge increases inversely with the amount of notice given. An additional option, to visit the contractors on site will be available, for a lesser charge. Any requests will be made in an e-mail stating: the box number, the required date, expenditure code, reason and if they are to be viewed on site or at the college, and thus accepted with arrangements for the box to be made available.

Boxes that are to be returned to storage will take up to one week, and as before, there is a response and delivery charge where the size of the charge increases inversely with the amount of notice. Additionally, a request must be made via email stating; the box number, the required date and expenditure code. The request will be acknowledged with arrangements by notification.

Upon the destruction of boxes, the relevant department will be notified one month prior to the destruction. Approval will be requested by e-mail and once received; arrangements will be made for confidential destruction from either site. Should a legislative or funding body change the storage criteria, please notify the Estates and Facilities Team with the relevant box numbers and information so that the record can b amended.

Whilst the Estates and Facilities team are responsible for arranging the safe storage of documents, it is important to note that departments and units are responsible for ensuring that they are compliant.

See appendix F for retention periods of specific information.

3.14 Responsibilities of Staff

All staff and authorised agents are responsible for:

- Checking that any data they provide to the College in connection with their employment are accurate and up to date.
- Checking that any data they provide to the College regarding learners or other third parties are accurate, fair and not excessive for the specific purpose of processing.
- Informing the College of any changes to the data in connection with their employment or to the data they provide regarding learners or other third parties.
- Checking any data that the College may send out from time to time giving details of information kept and processed about staff are accurate, relevant and not excessive. Staff should also advise the relevant data processor of any errors and/or omissions.
- Security of personal and sensitive data as set out about in 3.11 above.
- All SLT and CMT members are responsible for ensuring that their staff are aware of their obligations under the General Data Protection Regulations, and to ensure that only staff authorised by the SLT and CMT are permitted to process personal or sensitive data (Data Processors).
- All SLT and CMT members are responsible for advising the Data Protection Officer of any changes to the authorised data processor register in a timely manner.

3.15 Students Obligations

Students must ensure that all personal data provided to the College is accurate and up to date. They must ensure that the College is notified of any changes of address etc…

Students who use the College computer facilities to process personal data must comply with the Data Protection Act. Any student who required further clarification about this should contact their tutor or IT Helpdesk personnel.

Students who are under the age of 18 or who are deemed to be a 'vulnerable adult' (see Appendix K - Glossary of Main Terms), will be made aware that, as a condition of their enrolment, the College will ordinarily communicate with parents/carers regarding the following :

- absence from College (activities)
- academic progress
- any matters of concern

Signing the College enrolment form implies a student's consent to communicate with parents/carers. The College will ensure that this policy does not discriminate against those students under 18 who are not under the care of their parents e.g. for safeguarding purposes or those who choose to live independently. However, the College will endeavour to communicate with another interested party in lieu of a parent/carer.

Students can inform us they do not wish us to contact their parent/carer, to do so they must follow the process in appendix G.

3.16 Third Party Data

It may be necessary in some circumstances to disclose data which contain other third party data. Third party data in this case being data relating to any individual not directly related to the matter resulting in the need to disclose the information.

Where disclosure would reveal unrelated third party data the third party data be “redacted” (removed) from the data to be disclosed before disclosure takes place.

It is permissible to disclose third party data only with the written consent of the third party.

3.17 External Agencies

The day to day support of students will require, from time to time, the need to have contact with external agencies and organisations other than the College.

Where the College initiates contact with an external agency regarding a student, it should only do so with the knowledge and consent of the student. Exceptions to this apply where the College considers the health and safety of the student or that of any other individual may be at risk or where there has been a disclosure of a specific offence committed against property or an individual.

Where an external agency or other organisation contacts the college requesting information, in person, by phone or by email, no information should be disclosed in response to such an informal enquiry. Staff should explain that information cannot be released without a written request and that consent will be required from the student. The caller’s name and contact details should be taken so that the request can be passed on to the student who may wish to respond directly to the request.

3.18 Freedom of Information Act 2000

The College has a Freedom of Information Policy separate to this policy

The General Data Protection Regulations takes precedence over the Freedom of Information Act 2000 in instances where the rights of an individual under the General Data Protection Regulations would be contravened as a result of providing information under the Freedom of Information Act 2000.

3.19 Further Information

Contact the Data Protection Officer for further information regarding this GDPR Policy or the Freedom of Information Act 2000.

4 POLICY REVIEW

Change(s) Made	Reason for Change
Appendix J – change of date from 31st December 2030 to 2033	Changes to ESF contract

Review Date	Reviewed by:	Initial Approval by:	Final Approval by:	Next Review Date:	Review Period
Aug 2019	HR Business Partner	Head of HR and Organisational Development		Aug 2022	3 years
February 2020	HR Business Partner	Head of HR and Organisational Development	Audit Committee	February 2023	3 years
July 2020	HR Business Partner			February 2023	

Prepared by:	Authorised by:	Date:	Review Date:
HR Business Partner	Head of HR and Organisational Development	August 2019	August 2021

5 EQUALITY IMPACT ASSESSMENT

First Assessment Conducted by:	Date:	Final/Approved Assessment Conducted by:	Date:
HR Business Partner	August 2018	HR Business Partner on EDI committee	August 2018

6 PUBLICATION

Audience:	Published:
Staff	Staff Internet
	College Website

Appendix A

Data Protection - Security Advice

1. Introduction

The General Data Protection Regulations requires that personal and sensitive data processed by the data processors of the College are securely protected and stored.

This includes:

- Security for internal PC's and electronic data storage devices.
- Security of internal offices, rooms, desks, drawers, files etc.
- Security of data (Electronic or hard copy) when off site or in transit.
- Security of data when in use on PC's or in hard copy format from third party access.
- Transmitting data.

The advice within this section will assist data processors to protect College personal and sensitive data (Hereafter referred to simply as data).

2. Security Advice

2.1. Security for PC's and electronic data storage devices

All PC's, lap tops, black Berry's and any other device whether mobile or static must be secured with a password which is restricted to the sole user of that device. If shared access to any device is required all users must have authorisation (i.e. be registered to process data on the on the data processor register) to data on that device. Unsecured access or access to any individual who is not authorised will render a breach in GDPR security procedures and the security of any data accessible will be compromised.

Screens should be timed to lock out after a few minutes of inactivity to prevent access to any un-supervised screen data, or system's, by unauthorised personnel.

2.2. Security of internal offices, rooms, desks, drawers, files etc…

Any room where data are being used or stored must be capable of being locked when not in use. Furthermore, access to that room must be restricted to personnel who are authorised to process the data therein.

Where third party access is available or required within a room where data are being processed arrangements must be made to ensure that any third parties cannot see, and do not have access to any data being processed at that time.

All desk, drawers and filing systems must be capable of being locked with a key when the room is not occupied by authorised data controllers.

When data are finished with they should be securely stored and locked away (Whether electronic or hard copy format). A clear data policy must be adhered at all times when desks, work stations etc. are left unattended in unoccupied or otherwise secure areas.

2.3. Security of data (Electronic or hard copy) when off site or in transit

Mobile devices must be transported in a secure and lockable bag or case. No data should be transported off site unless it is adequately protected from theft, accidental loss (i.e. the device should be marked with a contact address or telephone number) or from damage (I.e.

in a water proof and solid container/bag etc.).

Data should not be left unattended in cars or on public transport. If it is absolutely necessary to leave for a short time any device/data in a car the device/data must be hidden, preferably in the boot and out of site.

When any data are stored off site (home, other offices, hotel rooms etc…) they should ideally be stored in a lockable room, cupboard, drawer, safe or deposit box, or stored securely and discreetly with the accommodation. The accommodation must be secured if the data are to be left in any unoccupied accommodation.

Be careful when viewing data on PC's or other forms of device as third parties may be able to see what is on your screen i.e. on trains whilst working next to an unknown person. The same is also the case when discussing personal data over the phone; be careful and aware of whom may be listening.

Appendix B **Staff Guidelines for Data Protection**

1. Many staff will process data about students on a regular basis, when marking registers, or College work, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through registration procedures, that all students give their consent to this sort of processing, and are notified of the categories of processing, as required by the GDPR.

   The information that staff deal with on a day-to-day basis will be 'standard' and will cover categories such as:

   • General personal details such as name and address
   • Details about class attendance, course work marks and grades and associated comments
   • Notes of personal supervision, including matters about behaviour and discipline.

2. Information about a person's religion or creed, gender, trade union membership, political beliefs, sex life or sexuality, health or criminal record is deemed sensitive data under GDPR. This can only be collected and processed with the person's consent.

   e.g. recording information about dietary needs, for religious or health reasons prior to taking students on a field trip; recording information that a student is pregnant, as part of pastoral duties.

   Whilst the person has the right to withhold such consent this may restrict the opportunities for the individual concerned.

3. All staff have a duty to make sure that they comply with the data protection principles, which are set out in the GDPR Policy. In particular, staff must ensure that records are:
   • accurate
   • up-to-date
   • fair
   • kept and disposed of safely, and in accordance with the College policy

4. The College will designate staff in each area as 'authorised staff'. These staff are the only staff authorised to hold or process data that is:

   • not standard data or
   • sensitive data

   The only exception to this will be if a non-authorised staff member is satisfied that the processing of the data is necessary:

   • in the best interests of the student or staff member, or a third person, or the College; AND
   • he or she has either informed the authorised person of this, or has been unable to do so and processing is urgent and necessary in all the circumstances.

   This should only happen in very limited circumstances. e.g. A student is injured and unconscious, but in need of medical attention, and a staff tutor tells the hospital that the student is pregnant or a Jehovah's witness.

5. Authorised staff will be responsible for ensuring that all data is kept securely.

6. Staff must not disclose personal data to any third party within the College unless for business academic or pastoral purposes.

7. Staff shall not disclose personal data to any third party outside the College except with the authorisation or agreement of a designated data controller, or in line with College policy.

8. Before processing any personal data, all staff should consider the checklist below:

Staff Checklist for Recording Data

- Do you really need to record the information?
- Is the information 'standard' or is it 'sensitive'?
- If it is sensitive, do you have the person concerned's express consent?
- Has the person been told that this type of data will be processed?
- Are you authorised to collect / store / process the data?
- Have you checked with the person concerned that the data is accurate?
- Are you sure that the data is secure?

If you do not have the person concerned's consent to process, are you satisfied that it is in the best interests of the student or the staff member to collect and retain the data?

Appendix C

Data Subject Access Request Form (General Data)

You should complete this form if you want the Calderdale College to supply you with a copy of personal data which we hold about you. You are entitled to receive this information under the General Data Protection Regulations.

We will endeavour to respond promptly and in any event within one month of the request.

Please supply clearly the following information:

Your full name:

……

Your address:

……

……

……

Your date of birth:

……

Your learner/staff number:

……

The Data you require:

Please provide a description of the sort of personal data which you are seeking and the dates from which we should search. If you want access to everything which we hold about you, please write "everything" but note that this will take longer to locate. We also reserve the right, in accordance with section 8(2) of the Act, not to provide you with copies of the information requested if to do so would take "disproportionate effort".

……

……

……

……

……

Please provide any further information which might assist us in our search:

……

……

……

……

Date of your most recent identical or similar request:

……

If you want to know answers to the following, please tick the boxes:

- why we are processing your personal data ☐
- to whom your personal data are disclosed ☐
- the source of your personal data ☐

If the information you request is of a confidential nature, we may contact you and ask you to provide further information to verify your identity. If we are not satisfied that you are who you say you are, we reserve the right to refuse to grant your request.

If the information you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that information. In certain circumstances we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision.

I confirm that I have read and understand the terms of this subject access form.

Signed…… Dated……

Please return this form to:

Data Protection Officer
Calderdale College
Francis Street
Halifax
HX1 3UZ

If you have any queries, please contact our Data Protection Officer on 01422 357 357 ext. 9515.

If, when you have received the requested information, you believe that:

- the information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware; or
- we may have passed inaccurate information about you to someone else;

then you should notify our Data Protection Officer at once, giving your reasons. The Data Protection Officer will then review the information and may amend your personal data in accordance with your wishes. Alternatively, the Data Protection Officer may notify you, giving reasons, as to why he believes the information which he holds about you is in fact accurate and relevant and is being processed for fair and lawful purposes.

Appendix D

Data Subject Access Request Form - (CCTV Data)

You should complete this form if you want the Calderdale College to supply you with personal data which may be held on CCTV tape. You are entitled to receive this information under the GDPR.

Requests for subject access for such access must be made within 31 days of the day for which subject access is required.

We will endeavour to respond promptly and in any event within one month of the request.

Please supply clearly the following information:

Your full name: ……..……
Your address: ……..……
…….
…….
…….
Your date of birth: ……..
Your learner/staff number: (If applicable) ……
Your precise location in/around the College.……..
A current passport sized photograph of you for identification purposes.

Please affix photo here

A detailed description of you for the time/date relevant to the subject access request.
……..……..
……..……..
……..……..
……..……..
……..……..
……..……..

A detailed description of what you were doing at the time/date relevant to the subject access.
……..……..
……..……..
……..……..
……..……..
……..……..
The exact time at which you were present in/at the location stated above.
……..……..
……..……..
We reserve the right, in accordance with the Act, not to provide you with copies of the information requested if to do so would take “disproportionate effort”.

The College will in all CCTV subject access requests seek a view from the Police that disclosure of an image subject to an access request, would not prejudice the "prevention or detection of crime", or the prosecution of offenders.

Please provide any further information which might assist us in our search:

- Date of your most recent identical or similar request:……..

If you want to know answers to the following, please tick the boxes:

- why we are processing your personal data ☐
- to whom your personal data are disclosed ☐

If the information you request is of a confidential nature, we may contact you and ask you to provide further information to verify your identity. If we are not satisfied that you are who you say you are, we reserve the right to refuse to grant your request.
If the data you request reveals details directly or indirectly about another person, we will have to seek the consent of that person before we can let you see that data. In certain circumstances we may not be able to disclose the data to you as this may involve disclosure of third party data (Annex III Data Protection Act), in which case you will be informed promptly and given full reasons for that decision.
I confirm that I have read and understand the terms of this subject access form.

Signed……..
Dated……..

Please return this form to: The Data Protection Officer
Calderdale College
Francis Street
Halifax
HX1 3UZ

If you have any queries, please call our Data Protection Officer on 01422 357357 ext. 9515

If, when you have received the requested information, you believe that:

- the information is inaccurate or out of date; or
- we should no longer be holding that information; or
- we are using your information for a purpose of which you were unaware; or
- we may have passed inaccurate information about you to someone else;

then you should notify our Data Protection Officer at once, giving your reasons. The Data Protection Officer will then review the information and may amend your personal data in accordance with your wishes. Alternatively, the Data Protection Officer may notify you, giving reasons, as to why he believes the information which he holds about you is in fact accurate and relevant and is being processed for fair and lawful purposes.

Appendix E

Mr/Mrs/Ms Smith
1 Any Street
Any Town
123 XYZ

Ref: DP****
Date

GENERAL DATA PROTECTION REGULATIONS: SUBJECT ACCESS REQUEST: FEES NOTICE

Dear Mr/Mrs/Ms
I refer to your request for access to information under the General Data Protection Regulations received on DD/MM/YYYY. Please note that there is a £XXXX fee payable for this service due to the size of the request.

Please make cheques payable to Calderdale College and return to:

Data Protection Officer
Calderdale College
Francis Street
Halifax
West Yorkshire
HX1 3UZ

Upon receipt of the fee and the request I will process your Data Subject Access Request. The College has one month to formally respond to your request.

Yours sincerely

Name
Data Protection Officer
enc

Appendix F **Guideline for Retention of Personal Data**

Note: This is not an exhaustive list. Medical records are kept for a variety of health and safety reasons, and will carry their own retention times

Type of Data	Suggested Retention Period	Reason
Personnel files included in training records and notes of disciplinary and grievance hearings.	6 years from the end of employment	References and potential litigation
Application forms/interview notes	At least 6 months from the date of the interviews	Time limits on litigation
Facts relating to redundancies where less than 20 redundancies	3 years from date of redundancies	Time limits on litigation
Facts relating to redundancies where 20 or more redundancies	12 years from date of redundancies	Limitation Act 1980
Income Tax and NI returns, including correspondence with tax office	At least 6 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993
Statutory Maternity Pay records and calculations	At least 6 years after the end of the financial year to which the records relate	Statutory Maternity Pay (General) Regulations 1986
Statutory Sick Pay records and calculations	At least 6 years after the end of the financial year to which the records relate	Statutory sick Pay (General) Regulations 1982
Wages and salary records	At least 6 years after the end of the financial year to which the records relate	Taxes Management Act (1970)
Accident books, and records and reports of accidents	3 years after the date of the last entry	RIDDOR 1995
Health records	During employment	Management of Health and Safety at Work Regulations 1999
Health records where reason for termination of employment is connected with health, including stress related illness	3 years	Limitation period for personal injury claims
Medical Records kept by reason of the Control of Substances Hazardous to Health Regulations 2002	40 years	COSHHR 2002
Student records, including academic achievements, and conduct	At least 6 years from the date the student leaves the College, in case of litigation of negligence. At least 10 years for personal and academic references, with the agreement of the student.	Limitation period for negligence

Appendix G

Contact with learners, their parents/carers procedures for withdrawal of consent

If you are a learner under 18 the College may contact your parents / carers and provide information about your conduct or progress. If you wish to opt out of this then you can do so at enrolment on the Privacy Notice or follow the process below and inform your parent / carer that you are doing so.

The withdrawal procedure will operate as follows:

- the learner informs the Progress Coach / Tutor / Course Leader that they wish to withdraw his/ her consent for College to contact their parents
- The Progress Coach / Tutor / Course Leader explains the implications of this to the learner
- The Learner completes the 'Withdrawal of Consent' form (Appendix H) in the presence of the Progress Coach / Tutor / Course Leader, who also needs to sign it
- This document will then trigger a standard letter (Appendix I) which will be send out to the parent / carer.
- The Progress Coach / Tutor will confirm with the learner the appropriate contact details which are to be held centrally, for direct contact with the learner and emergency contact details. If there are any amendments these need to be recorded on the relevant systems.

Appendix H **Withdrawal of Consent Form**

Learner withdrawal of consent to contact parents / carers

I wish to exercise my right to receive directly, all information about my academic progress, together with any other matters relevant to me being a student at college.

Any requests for information from other family members should not be agreed to without my approval.

I understand that the exercising of this right also makes my actions my personal responsibility and I undertake to fully comply with the Student Charter and Code of Conduct.

I also understand that, if I also withdraw consent for my parents/carers to act as my emergency contact in the event of an emergency or ill health, I must provide an alternative. The individual named as the emergency contact should know that they have been named and confirm that they are happy to act in that capacity. Full details will need to be provided so that they can be added to our central information systems.

Name of Learner: ……. (Please print full name)

DOB: ……..

Student Ref : ……..

Signature of Learner: ……

Date: ……

Name of Progress Coach / Tutor …… (Please print full name)

Signature of Progress Coach / Tutor: …….

Date: …….

This form must be handed to your Progress Coach. A letter will be issued to your parent/carer explaining that we will no longer be making contact with them. The process is not valid until this letter has been issued by the college.

Please note: If you are a Work Based Learner, the College will continue to pass relevant information to your employer.

Appendix I Follow up letter to be sent to parents/carers

Date

Parent/Carer of:

«AddressBlock»

Dear Parent/Carer

Your son/daughter, «Firstname1» has informed us that they are withdrawing their consent for the College to contact you further and they have completed the relevant documentation to confirm this. Consequently all future communication from college will be sent directly to them. As part of the General Data Protection Regulations, we are obliged to comply with your son/daughter's request.

It may be that your son/daughter wishes us to retain your contact details as an emergency contact; please confirm this with them. If he/she chooses and alternative emergency contact in the event of an accident or ill health, the individual named as the emergency contact should know that they have been named and confirm that they are happy to act in that capacity.

We do hope «Firstname1» will continue to keep you informed of his/her progress at all times.

Yours faithfully

Name
Job Title / Department

Appendix J - GDPR and ESF
Department for Work and Pensions (DWP) ESF Managing Authority is the controller for all personal data required to help deliver the ESF programme under the terms of its ESF Funding Agreement. Some organisations may collect other/additional data about their participants that is not essential for delivering the ESF programme. The ESF Managing Authority is not the controller for such additional data. In this scenario, individual organisations must ensure they understand and are compliant with their responsibilities under GDPR as the data controller.

ESF Data Retention Periods
The requirements for data retention for ESF projects remain the same. All supporting evidence must be retained along with evidence relating to invoice(s), management information and all other documentation relevant to delivery of the subcontract (including state aid forms) until at least 31 December 2033.

The lawful basis for controlling or processing personal data under ESF
The DWP ESF Managing Authority, will be processing personal data in the ESF programme according to the following lawful basis - **Article 6 (1) (e) GDPR** 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'.

The lawful basis for controlling or processing `special category' data under ESF (e.g. health, ethnicity)

Article 9(2) (b) GDPR
This article of the GDPR provides DWP with the lawful basis for processing `special category' (sensitive) data:
"processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment** and **social security** and **social protection law** in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;"

ESF participants **cannot** claim the following rights in terms of ESF personal data:

- Right to erasure ("right to be forgotten")
- Right to portability of their data

However, individuals do have a right to object to their data being processed.

Privacy notices relating to ESF
Projects will need to make use of DWP's privacy notice as published in the DWP's personal information charter for all ESF personal data only. ESF participants should also be made aware of the contents of the DWP's personal information charter in relation to all ESF personal data held about them (and this should include a web link or similar to the full site). The URL for the DWP personal information charter is www.gov.uk/dwp/personal-information-charter

Appendix K

Glossary

GDPR:	General Data Protection Regulations
CoP:	Code of Practice
SLT:	Senior Leadership Team
CMT	College Management Team
ICO	Information Commissioner's Office

Key definitions as determined by the ICO

Data:	Means information which- a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, b) is recorded with the intention that it should be processed by means of such equipment, c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, d) does not fall within paragraph a), b) or c) but forms part of an accessible record or e) is recorded information held by a public authority and does not fall within any of paragraphs a) to d).
Personal data:	Means data which relate to a living individual who can be identified- a) from those data, or b) from those data and other information which is in the possession of, or likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Sensitive personal data:	Means personal data consisting of information as to- a) the racial or ethnic origin of the data subject, b) his political opinions, c) his religious beliefs or other beliefs of a similar nature, d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992), e) his physical or mental health or condition, f) his sexual life, g) the commission or alleged commission by him of any offence, or h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.
Processing:	In relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the data, including- a) organisation, adaptation or alteration of the information or data, b) retrieval, consultation or use of the information or data, c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

	i) alignment, combination, blocking, erasure or destruction of the information or data.
Data Subject:	Means an individual who is the subject of personal data.
Data controller:	Means … a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.
Data processor:	In relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.
Inaccurate data:	For the purposes of this Act data are inaccurate if they are incorrect or misleading as to any matter of fact.
Recipient:	In relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.
Third party:	in relation to personal data, means any person other than – a) the data subject, b) the data controller, or c) any data processor or other person authorised to process data for the data controller or processor.
Vulnerable Adult	Defined within 'No Secrets'* guidance as a person: "who is or may be in need of community care services by reason of mental or other disability, age, or illness; **and** who is or nay be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation". **No Secrets – Department of Health 2000 Ref: Safeguarding Adults: The role of heath service managers and their boards DoH Social Care Policy 14 Mar 2011.*