Data Protection Policy

CALDERDALE COLLEGE
INSPIRING LEARNERS TO SUCCEED IN LIFE & IN WORK

Data Protection Policy

CALDERDALE COLLEGE
INSPIRING LEARNERS TO SUCCEED IN LIFE & IN WORK

1.0 General Information

1.1 Policy Statement

The objective of this policy is to ensure that:

- all members of staff (authorised data processors) are familiar with their obligations under the Data Protection Act (DPA) 1998.
- all data processing carried out by the College complies with the DPA and in line with the eight data protection principles, the registered purpose groups and the DPA 1998.

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

1.2 Responsibilities

- **Dedicated Data Controller**: Head of Human Resources
- **College Leadership & Management Team (CLMT):** To ensure that Data Processors and agents within their own area are fully aware of their obligations under the DPA 1998 and this policy to ensure compliance with the law.
- **Data Processors:** (All Staff) - To be fully aware of their responsibilities under the DPA 1998 and 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.

Compliance with this Policy and CoP will be subject to internal and external audit. It is therefore the responsibility of all CLMT members to ensure that their own area Data Processors and agents are fully aware of their obligations under the DPA 1998 and this policy to ensure compliance with the law.

Failure to comply with the DPA 1998 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.

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 controller initially. If the matter is not resolved it should be raised as a formal grievance.

1.3 Potential impact on Equality, Diversity and Inclusivity

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.

2.0 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 Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act). The DPA gives people specific rights in relation to their personal information and also place certain obligations on organisations that are responsible for processing personal data.

Personal data is defined as being data which relate to a living individual who can be identified:

- from those data: or
- from those data and other information which is in the possession of, or is 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 person in respect of the individual. *(Information Commissioners Office (ICO)*

The DPA 1998 sets out eight Data Protection Principles which dictate how all data processing should be executed, in summary these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
- Be adequate, relevant and not excessive for those purposes.
- Be accurate and kept up to date.
- Not be kept for longer than is necessary for that purpose.
- Be processed in accordance with the data subject's rights,
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

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 Data Protection Policy [DPP].

3.0 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 8 purpose groups.

In order for the College to process lawfully under the DPA 1998 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 College Data Controller immediately. Additional purpose groups can be requested to be included on the College Data Protection Registration from the ICO. The College Data Controller 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 College Data Controller.

4.0 Codes of Practice (CoP)

To ensure compliance with the DPA 1998 Calderdale College has established a CoP system. Familiarity and understanding of the CoP will ensure that all College data processors and agents of the College contribute effectively in complying with this policy and the DPA 1998.

4.1 The Data Controller and Data Processors

The Data Controller

The College as a corporate body is the "Data Controller" under the DPA 1998, and the College is therefore ultimately responsible for the implementation of the DPA 1998. However, the designated College Data Controller will deal with day-to-day matters on behalf of the College.

Calderdale College's Data Controller is the Head of Human Resources.

Data Processors & Data Processor Registration

All CLMT members must register with the Data Controller. The College must hold a list of all personnel and agents authorised by their respective departments to process personal and sensitive data where relevant. Each CLMT member must ensure that the data processor register for their department is accurate and up to date. Failure to update the register will result in a failed Data Protection audit. Furthermore, failure to prevent unauthorised users from accessing personal data may lead to legal sanctions (personal and corporate) under the DPA1998 Act.

All data processors must:

- know and understand the data protection principles.
- know and understand the purpose groups relevant to their department.
- only process data, or be allowed access to data, which are covered by their departmental purpose group.
- have read and signed to indicate understanding and acceptance of the College data protection policy and allied policies and procedures.
- undergo DPA (And Freedom of Information Act 2000) training.

4.2 Sensitive Data

Sensitive data are data that refer to (amongst others) a person's health, gender, religion, family status or criminal record. Departments within the College will from time to time have legitimate reason to process sensitive data. By the very nature of this data and as it is recognised that processing of sensitive data could cause concern or distress to individuals, staff and learners will be asked for express consent for the College to process sensitive data. Offers of employment or course places may be withdrawn if an individual refuses consent.

4.3 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 DPA 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.

4.4 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 DPA is referred to as a “Data Subject Access Request”.

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

The College has 40 working days (from the first full day following the request) to formally respond to any data subject access request.

In the case of a CCTV data subject access request (Appendix D) the College Data Controller 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 College Data Controller. The Data Controller will forward to the applicant a fee request notice (where applicable) 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 College Data Controller.

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 College Data Controller.

The College Data Controller 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 CLMT member to ensure that the College meets the deadline obligations set out in the Data Protection Act 1998 (40 working days).

The College Data Controller 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.

A data subject access request administration fee of £10.00 will be levied for all subject access requests by external parties.

In exceptional circumstances, the College reserves the right to waive a data subject access fee in respect of a current staff member, learner or former learner. Discretion for waiving a data subject access fee is with the Data Controller.

4.5 College Data Retention

All College records, whether they contain personal, sensitive or any other type of information not covered by the DPA 1998 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.

4.6 Notification of Data Processed and Held

All Staff, learners and other users are entitled to know:

- What data the College holds and processes about them and why
- The reasons for the College holding this data
- How to gain access to it
- How to keep it up to date
- What the College is doing to comply with its obligations under the DPA 1998

- The College will make available a standard form of notification. This will advise of the data that the College holds and processes about staff and learners, and the reason for which it is processed.

4.7 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 4.3 above.
- All CLMT members are responsible for ensuring that their staff are aware of their obligations under the Data Protection Act 1998, and to ensure that only staff authorised by the Assistant Principals or Head of Units are permitted to process personal or sensitive data (Data Processors).
- All CLMT members are responsible for advising the College Data Controller of any changes to the authorised data processor register in a timely manner.

4.8 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 J - 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.

4.9 Consent to Process Data

Calderdale College will obtain express consent from all staff to process sensitive data regarding their employment at the College.

The processing of personal staff data will be as set out in this policy. Learners are deemed to have consented to the processing of personal and sensitive data on completion of the enrolment process. Offers of employment or course places may be withdrawn if an individual refuses consent.

4.10 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.

4.11 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.

5.0 Freedom of Information Act 2000

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

The Data Protection Act 1998 takes precedence over the Freedom of Information Act 2000 in instances where the rights of an individual under the Data Protection Act 1998 would be contravened as a result of providing information under the Freedom of Information Act 2000.

6.0 Further Information

Contact the Data Controller for further information regarding the College Data Protection Policy, the DPA 1998 or the Freedom of Information Act 2000.

7.0 Appendices

A. Security Advice
B. Staff Guidelines for Data Protection
C. Data Subject Access Request form (general data)
D. Data Subject Access Request form (CCTV)
E. Fee Request Letter
F. Guideline for Retention of Personal Data
G. Contact with learners, their parents/carers – procedures for withdrawal of consent
H. Withdrawal of consent form
I. Follow up letter to be sent to parents/carers
J. Glossary of terms

CALDERDALE COLLEGE
INSPIRING LEARNERS TO SUCCEED IN LIFE & IN WORK

Appendix A

Data Protection Act 1998 - Security Advice

1. Introduction

The Data Protection Act 1998 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 DPA 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 1998 Act.

   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 DPA 1998. 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 Data Protection 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 Data Protection Act 1998.

You should send a cheque in the sum of £10 made payable to Calderdale College. We will endeavour to respond promptly and in any event within 40 days of the latest of the following:-

- your cheque clearing; or
- our receipt of this request; or
- our receipt of any further information from you which is required to enable us to comply with your 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:

The Data Controller - HR
Calderdale College
Francis Street
Halifax
HX1 3UZ

If you have any queries, please call our Data Controller on: 01422 339 311

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 Controller at once, giving your reasons. The Data Controller will then review the information and may amend your personal data in accordance with your wishes. Alternatively, the Data Controller 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 Data Protection Act 1998.

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

You should send a cheque in the sum of £10 made payable to the Calderdale College. We will endeavour to respond promptly and in any event within 40 days of the latest of the following:-

- your cheque clearing; or
- our receipt of this request; or
- our receipt of any further information from you which is required to enable us to comply with your 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 section 8(2) of 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

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

DATA PROTECTION ACT 1998: SUBJECT ACCESS REQUEST: FEES NOTICE

Dear Mr/Mrs/Ms

I refer to your request for access to information under the Data Protection Act 1998 received on DD/MM/YYYY. Please note that there is a £10 fee payable for this service.

Please complete the enclosed Data Subject Access Request form and return it with your payment to:

Head of Human Resources (Data Controller)
Calderdale College
Francis Street
Halifax
West Yorkshire
HX1 3UZ

Please make cheques payable to Calderdale College.

Upon receipt of both the fee and the request form I will process your Data Subject Access Request. The College has 40 working days to formally respond to your request.

Yours sincerely

Name
Head of Human Resources (Data Controller)
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 a learner is 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 enrolement 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 student and emergency contact details. If there are any amendments these need to be recorded on the relevant systems.

Appendix H **Withdrawal of Consent Form**

Student 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 Student: ……. (Please print full name)

DOB: ……..

Student Ref : …….

Signature of Student: ……

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 Data Protection Act 1998, 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

Glossary

DPA:	Data Protection Act 1998
CoP:	Code of Practice
CLMT:	College Leadership & 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 as defined by section 68, 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.*