Data Protection Policy

Document Controls:

Document Name: - Data Protection Policy

	Name	Title	Last Revised	Next Review
Owner(s)	Gary Horne	Executive Vice Principal: Finance & Corporate Development	06/10/2017	30/9/18

Revised by	Date	Changes	Approved	Version
GH	24/7/2016	Updates from Management feedback		V1.0
GH	18/8/2016	Further updates from Management feedback		V1.1
GH	06/10/2017	Full text review and update. Definition of Personal and Sensitive personal data as agreed by GDPR CG	CE	V1.2
GH	05/11/2017	Breach reporting requirements and guidance	CE 07.11.17	V1.3
GH	10/12/2017	Encryption requirements, staff responsibilities, data controllers	SLT 12.12.17	V1.4

Introduction

Colchester Institute needs to retain information about its staff and students to allow it to carry out its day to day business activities and deliver its strategic objectives, as well as meet legal obligations including data requirements of funding agencies and statutory bodies.

The lawful and correct treatment of personal information is of paramount importance to the organisation and to maintain confidence with all our stakeholders, whoever they are in the wide range of activities we undertake. Through dissemination of this policy we will ensure that the College treats all personal information, including sensitive personal information lawfully and correctly.

To comply with the provisions of the Data Protection Act 1998 (The Act), the College takes steps to ensure that personal information is collected only where necessary and is used in accordance with the Data Protection Principles which state that personal data must be –

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary;
- processed in accordance with individual's rights;
- held as securely as possible
- not transferred to countries without adequate protection.

Purpose

The purpose of this policy is to ensure that everyone handing personal information is:

- Aware of the the Data Protection Act 1998
- Complies with data protection procedures; and
- Ensures that data subjects within their area of management or control are aware of their rights under the Act.

Definitions and interpretation

Scope (information covered by the Act)

'Personal data' covered by the Act is essentially any recorded information (paper and electronic) which identifies a living individual. Personal data held by Colchester Institute will include contact information for a variety of stakeholders and other personal details.

Personal Data

To identify an individual, Colchester Institute considers 'Personal data' to be:

- *The name of an individual plus any one of the following:*
- *Date of Birth, Home address, National Insurance Number, Bank Account Details, telephone contact information, next of kin, personal location data e.g. IP address, or any other unique identifier*

Sensitive Personal Data

Furthermore, in accordance with the Act, Colchester Institute considers 'Sensitive Personal Data' to be any information relating to an individual's *racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health, care needs, care status, physical disabilities, medical, geometric or biometric data, sexual life or details of criminal convictions or any other data of equivalent personal standing.*

Responsibilities

In order to respond to the requirements of the Act, Colchester Institute will:

- fully observe conditions regarding the fair collection and use of information
- meet its legal obligations to specify the purposes for which information is used
- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- ensure the quality of the information used e.g. accurate and relevant.
- hold personal information on Management Information Systems for as long as is necessary for the relevant purpose, or as long as is set out in any relevant contract held by the College and in the *Retention of Records Policy* (this document defines which records should be kept and for how long).
- ensure that the rights of people about whom information is held can be fully exercised under the Act (these include: the right to be informed that processing is being undertaken; the data subject's right of access to their personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as wrong information)
- take appropriate technical and organisational security measures to safeguard personal information and
- ensure that personal information is not transferred without suitable safeguards.
- report any breach or loss of personal data to the Information Commissioner's Office (ICO) in accordance with the ICO's prescribed procedures.

Processes

All personal data will be obtained, as far as possible, from the individual and processed on the basis of informed consent. Personal data must not be obtained by any means, which mislead or deceive. Therefore, all requests for consent will be in plain language, specific to the person being addressed and clearly state the purposes for which the data is being obtained.

- Personal data will only be collected for justified reasons and specified purposes. These will normally be communicated, in advance, to the person concerned.
- Sensitive personal data information may normally only be processed if the person has given their explicit consent. Personal data processed should be accurate, valid and restricted to that which is necessary to satisfy requirements.

Important

The security of employee and student data should be comprehensively protected against unauthorised access, improper use, accidental loss, destruction and/or damage, by being kept in locked storage, password protected, or by using other suitable precautions.

Electronic Sensitive Personal Data must be password protected and/or encrypted. External hard drives, memory sticks, unencrypted laptops and personal cloud storage must not be used to store sensitive data. Staff must take all precautions necessary to maintain confidentiality of all such information whilst in their possession, whether in soft copy or hard copy. The IT Security policy must be followed at all times.

Personal information should not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party. Staff should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered

Information on authorised access and disclosure for students is included on the College

enrolment form. All staff must ensure they confirm any disclosure is authorised and ensure they follow appropriate processes. (Appendix B "Procedure for Police Enquiries/Attendance on Site)

Colchester Institute will ensure:

- all staff are aware of the data protection act and will ensure Colchester Institute's policies and procedures comply with these principles.
- all staff are aware of what to do in the event of discovering an actual or suspected breach or loss of information
- everyone managing and handling personal information understands that they are responsible for following good data protection practice
- this policy is available to every member of staff via college portal
- everyone managing and handling personal information is appropriately trained and supervised
- queries about handling personal information are promptly and courteously dealt with and clear information is available to all staff
- any changes to the policy will be communicated and staff training will be provided where necessary.

Obligation of Staff

- Staff should be aware of the Act and how the rules apply to them.
- Staff must complete data protection induction and training
- Staff have a responsibility to ensure that they respect confidential information in their possession and maintain information security. Unauthorised disclosure of confidential information to a third party, or assisting others in disclosure, will be viewed by Colchester Institute with the utmost seriousness.
- Staff must assure themselves that any personal data being disclosed is done so for a legitimate business purpose and that the person or agency in receipt of such information is entitled to receive it.
- Where authorised to disclose information, staff are responsible for ensuring that all personal data provided supplied is accurate and for notifying any errors or changes as these arise
- Staff are responsible for ensuring information is kept no longer than necessary and held in accordance with the retention of records policy.
- Staff will ensure measures are taken to lock computers when not in use, and prevent monitors from being viewed by others if used in open access areas where personal data could be viewed.
- Information containing personal or sensitive personal information will not be left out on desks where it can be viewed and cleared from desks at the end of each working day.
- Staff will immediately report any breach or suspected breach or loss of personal information as detailed below.
- Staff must not use personal cloud storage, external hard drives, memory sticks or any other unencrypted devices (eg laptops) to store or transfer sensitive data.

Obligation of students

- Ensuring personal data provided to the College is accurate and up to date
- Notification of any errors or changes as these arise e.g. changes of address

Technical Security

The College has in place appropriate security measures as required by the Act. Information systems are installed with adequate security controls and all employees

who use these systems will be properly authorised to use them for College business.

The *IT Security Policy* will be published on the College portal. The College relies on computers to store data, and will maintain up-to-date antivirus software and appropriate firewalls. Regular back-ups and robust processes for disabling accounts as people leave. Accounts are controlled via groups to ensure only those that need to know certain information have access to that information. A *Mobile Device Acceptable Use Policy* covers mobile security access control. The wireless access points used at the College all require authentication to be used and cannot be accessed by unauthorised persons. The College ensures all emails are scanned with an industry scanning software. Staff training records will be maintained by HR.

Designated Data Controllers
The College has designated Data Controllers with responsibilities for employee and student records as follows: -

Human Resources Manager - employee records
Director of Funding and Information - student records

Breach Reporting
The College is required to notify the ICO in the event of a data security breach. Any staff member who is concerned about data loss via hard copy or soft copy form must immediately contact the College's nominate Data Protection Officer (DPO). This is the Clerk to the Corporation. Contact details are reproduced below:

Email: hazel.paton@colchester.ac.uk
Tel: 01206 712606

The Data Protection Officer will investigate the concern from the details provided. The person reporting the breach must provide as much information as possible in order for the investigation to take place. The DPO will involve Data Controllers and members of the College Executive as required. The outcome of the investigation will determine whether there will be a requirement to report the breach to the ICO under relevant guidelines. https://ico.org.uk/media/1536/breach_reporting.pdf

Entitlement to Access to Personal Data
Employees and students are entitled to make a formal request to access any personal data which is being used or "processed" by a computerised system and personal information kept about them as part of a "relevant filing system". Requests must be made in writing as stated below. The College aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within 40 days of the request.

Employees
Employees wishing to access such personal data must do so in writing to the Human Resources Manager (Data Controller – employees).

Students
Students wishing to access such personal data should complete the Access to Personal Data form (see Appendix A) which is also available from the Registry Department. The College will make a charge of £10 for each occasion a request for access is made.

Sharing information with parents

The student declaration on their enrolment form includes the statement "I understand that Colchester Institute may contact my parent/guardian regarding my attendance, progress, achievement, wellbeing, welfare and personal safety until the end of the academic year in which I turn 18 years of age", which provides consent for us to share appropriate information, including following up attendance, sending reports home and discussions at parent events.

If a parent/guardian of a student in this age range requests information about their son or daughter than this can be released provided they are named as the next of kin on EBS or ProMonitor and that the member of staff releasing the information has taken steps to ensure the authenticity of the enquirer, and the accuracy of the information given. To eliminate errors as many checks as possible relating to the subject of the inquiry must be made, e.g.

- Full name (not just initials)
- Spelling of name
- Address
- Date of birth
- Course attended
- Next of kin – name and address / phone number

If the staff member is not satisfied that the enquirer is not genuine, or the named next of kin, then they must not release the information.

A student can provide up to date information about their next of kin at Registry or one of the Information Centres.

Students 19 and over

No information can be shared with the parent/guardian of a student aged 19 or overwithout the express consent of the student.

See Appendix A, Procedures for the Release of Student Data for more information, including requests from individuals or agencies

Any other requests for information from external agencies should be referred in the first instance to Registry for action under these procedures.

Any query regarding the implementation of this procedure or if individual cases occur where a member of staff is uncertain, reference must be made in the first instance to the relevant Data Controller. In no circumstances should students or other enquirers be given private addresses or telephone numbers of staff or other students.

College Publications

Personal information in the public domain for genuine business purposes, such as names, job titles, etc. included in marketing publications, telephone directory, notice boards, is exempt from the Act. However, any employee or student who has good reason for wishing to be excluded from such public information should contact the relevant Data Controller.

Use of CCTV

The College's Closed Circuit Television Code of Practice complies with the ICO's

CCTV Code of Practice and is the responsibility of the Facilities Manager. Please refer to the Colleges *CCTV Code of Practice*

Disposal of Confidential Waste

Employees must ensure that they dispose of all personal and sensitive data securely. E.g. Using the confidential waste bags or shredders. Documentation containing sensitive personal data must be kept secure whilst waiting to be confidentially shredded (eg Shredding sacks half-filled must be locked away). No documentation containing sensitive personal data will be placed in waste paper or re-cycling bins.

Other Relevant / Associated Policies Documents:

- *CCTV Code of Practice*
- *IT Security Policy*
- *Mobile Device Acceptable Use Policy*
- *Retention of Records Policy*
- *Staff Disciplinary Policy*

Appendix A

Procedures for the Release of Student Data

DISCLOSURE OF INFORMATION

Colchester Institute is registered under the **Data Protection Act 1998**. It is an offence under the above Act, which relates to all data, to use, reveal or publish such information other than in accordance with the registration of Colchester Institute.
(Taken from the Disclosure of Information policy, Colchester Institute)

We currently follow a service standard of 5 days for the release of data, this is often only 2 days during less busy times of the year. Letters can only be produced and can be collected from Registry, if this is not possible for them to be collected then it can be sent to the address held on EBS for the student. If the student has moved and not informed us previously, this must be changed before the letter can be produced.

Data release for students under the age of 18 is possible if the request is from the NOK, employer, police or governmental body. If anyone requests the release of data for 18+ students and they are not the student, (except for Employers that are sponsoring the student – see page 4) **nothing can be revealed without the students' permission**. No mention of whether the person is even a student with us, be very aware as it is very easy to do if you have the information in front of you.

WHERE DO REQUESTS FOR STUDENT DATA COME FROM?

Colchester Institute receives many requests for the release of student data, the most common requests come from the following sources:

- **STUDENTS, PARENTS/GUARDIANS**
- **GOVERNMENT AGENCIES:** Jobcentre Plus, Child Benefit, UK Border Agency, Child Support Agency, Council Tax, Tax Credits, Home Office
- **POLICE:** follow separate procedure (see page 5)
- **SOLICITORS:** follow separate procedure (see page 4)

HOW DO STUDENTS AND THIRD PARTIES REQUEST INFORMATION?

STUDENTS

Current students should request confirmation of their student status from Registry. A student can make their request in writing/email or complete a **Permission form for the Disclosure of Information**. If they are a current active student 19 yrs or under or on a HE course, they can be checked and printed at the counter while they wait. Go to enrolments and click the arrow for council tax, check that the details are all correct and print copy on headed paper for the student.

Past students who require their data for benefit purposes must make their requests in writing. Other requests from past students such as references should be referred to Academic Standards (Kevin Hewes). Ext: 2223, Room A2, kevin.hewes@colchester.ac.uk.

Application Enquiries

Pass to Admissions, we can only release details for an enrolled student, for the enrolments they have had, past and present.

PARENTS/GUARDIANS

Parents/guardians can request information regarding attendance, progress & achievement if they are the named 1st & 2nd next of kin. This is possible until the end of the academic year in which the student turns 18 years of age. If the student is 18 years or over, then **permission** from the student is required.

THIRD PARTIES

Third parties must make their request in writing. Where possible the **consent** from the student must be obtained. See section on checking authenticity for further details. If no authorisation is possible, then, no information may be released – not even to say a person is not an enrolled student here.

EMPLOYERS

If an employer requests details of attendance, progress or achievement, this is possible for those sponsoring the student. The employer will have to request this in writing in the normal way. Do the normal authenticity checks before releasing this information. Always keep the details of information released on file in the data release folder.

SOLICITORS (charge of £10 – for each Subject Access Request)

When solicitors request data for a student, firstly you must get authority from the student before releasing any information, most solicitors will enclose a signed consent letter from the student in question. Then follow the request, they will all be different. Some will just need dates or attendance and others may want all the student data held by us. If all data held is required you need to contact the following areas for this information: The students Tutor, CMG for the students subject area, Helen Joynes, Steven Carter. If they are a HE student Chris Mills & WBL Michelle Tyler also needs to be asked. We have 40 days from the day of receipt of the fee and letter of consent to complete these requests. If the reply is to be emailed, then the emails must be passworded, for those sent by post to be signed for. (Special delivery - Ask the postman to do this for you). If they pay by cheque this can go through Bill Till and hand written receipt can be sent with the release letter and paperwork when it is sent out.

CHECKING AUTHENTICITY AND ACCURACY

Every reasonable step must be taken to ensure the authenticity of the person/company requesting the release of information.

AUTHENTICITY Students – please request the following information to ensure the identification of the student:

- Name
- Student Number or Date of Birth
- Address

Request further information from the student if you are unable to obtain all the details you require or if you need further proof of identification.

Third parties – please request the following information:

- Name of the organisation/company including a contact name if possible
- Address of the organisation/company including a contact phone number if possible (google as a check for authenticity)
- Student information i.e. name, date of birth, address, course of study
- Reason for the release of information
- Authorisation in writing/email from the student

ACCURACY

To ensure the correct identification of the student in question check the information you have been given against the information held by Colchester Institute. If the information does not match do not release any details until you have confirmed *correct identification.*

Student Loan Company

Student signs the Authority for this information to be given on their Enrolment form, this would be requested from the HE Registry Assistants.

HOW TO ACTION A REQUEST FOR THE RELEASE OF STUDENT DATA

STEP ONE – obtain your request in written format

REQUESTS FROM STUDENTS - Obtain your request in written format, permission form for the disclosure of information or by email. In certain circumstances you may complete a permission form for the disclosure of information if a student is unable to. However, you must ask relevant questions i.e. name, DOB, address etc to check their identity.

BACP - Letter for counselling students wishing to register with the BACP.

Template see page 11. & in Q:drive/Curriculum,/Planning & Quality/Funding & Information/Registry/All Data release Information/templates for data release letters.

REQUESTS FROM COUNCILS/PENSION COMPANIES – On occasions we are asked to complete pre-printed letters from some councils and other companies such as pensions or carers. These will ask for the same information as usual but maybe hours for placement, out of class, course work. Contact the tutor for this information by email, so we can keep a copy and attach to a copy of the completed form and file in the usual place with all other release documents.

REQUESTS FROM SPONSERS/EMPLOYERS - If they request information for the student they are sponsoring (they have to be paying the fees), obtain your request by letter/email. Request original letters on headed paper where you need to prove the authenticity (via google etc.) of an organisation. They are entitled to information regarding their attendance, progress and achievement.

REQUESTS FROM THE POLICE - Before giving out any information to the Police, we need to have a

completed A101 form (from Essex Police). Any other Police force will have their own equivalent form (for Disclosure of personal details for the use of investigating a crime). Always check that the form is signed by an Officer. Then gather all the relevant info and confirm with a *College Executive* who can give the authority to release the information. Details can only be released if the student is enrolled. Then follow the normal procedures. If the student is suspected of a crime that is deemed of a violent or sexual nature, or where staff & students may be at risk, the Police must let us know if there is a safeguarding issue. Screen shots can be used from EBS central if all contact info. is requested. Keep a copy of all information released, the email and A101and keep in the blue folder in the safe. Complete the front sheet in the front of the blue folder for each one released. If no information can be released enter the details on the spread sheet in the front of the blue folder in the safe.

STEP TWO – check authenticity and accuracy
Records can be checked against EBS.

STEP THREE – date stamp the request

STEP FOUR – search for student information

PERSONAL DETAILS, STUDENT COURSE DETAILS AND FEES

EBS4 Client will detail the following:

- Personal details
- The course the student is enrolled on
- Fees that have been paid including any waivers applied to a student's course fees

Curriculum found in **EBS4** details course information including:

- Course fees
- Teaching staff
- The number of hours taught each week (To be collated from the registers)

ATTENDANCE DETAILS

You must look at the Registers to check a student's attendance. Registers can be found in Ontrack and search for student's number and go to Registers in the left hand column.
If the registers are not completely up to date, email the course tutor and request confirmation of attendance. Keep a copy of the email with the student's data request.

If the attendance is requested, go to the register, top right hand corner and click on the green icon, this will bring up attendance register report. Calculate using the total of each mark at bottom right hand side.

To calculate: **Actual attendances**

Possible Attendances x 100

START & END DATES:

- Start date of a course – the registers will indicate the start date.
- Start date of an individual – again the registers will show their first attendance.
- End date of a course – if the course is completed use the register or if the student is still in attendance you can use an expected end date and put the last day of term.

In some instances a student may request the percentage of their attendance. Follow for the report:

Any problems in gaining this information via the link, contact **Timetabling & E-Registers**, they will be able to provide you with a print out.

STEP FIVE – complete your paperwork

Once you have gathered all the relevant information complete your request. There are various folders for storage on the Q Drive: *Curriculum, Planning & Quality/Funding & Information/Registry/All Data Release* Information - non-standard letters in *Data Release letters* by year and *Data Release Tally* by year for every letter released.
If the students are 16 -18 or on a full time HE Course, they can then be printed out from the counter tills. Go to enrolments screen and bring down the council tax check list/preview council tax/ if all the information is correct according to EBS, print out the certificate on headed paper.

These can be printed for Gym membership, doctor/dentist, banks, musicians union, etc. as well as Council Tax. Any other requests for certificates for Tax credits, Housing or any other benefits must be passed to Jayne for individual certificates.

If the information is incorrect, pass the request to Jayne to print an individual letter.
If the student requires a letter for Tax credits/Housing benefits or any other including hours, needed, there is tax credits template in reports-*Portal/Information Systems/CI Reports/Registry/*Tax credits letter.
If the letter is for the council then go to *Portal/Information Systems/CI Reports/Registry/*. *Portal/Information Systems/CI Reports/Registry*/Council Tax Report by Learner.

Requests from third parties or any Subject data release that is out of the ordinary must be checked and approved by the Director of Funding and Information (Julie Cox) or other member of CMG, before any information is released.

Tracking Data Released - Each letter released is tracked on the following tracking sheets, this is to keep all the information by Student number/Name/Reason for release/how it was sent or collected. This ensures we have a record for every letter released for each student and why. The Tracking sheets by year for Data release is on:

- Q:drive/Curriculum,/Planning & Quality/Funding & Information/Registry/All Data release Information

Keeping copies of paperwork - If certificates can be printed at the counter, print one copy on headed paper Stamp and sign (pp) and give to the student. If it is not possible, ask the student to complete a data release request, a record of your response from any emails from tutors. File in the Data Release folders (bottom drawer end filing cabinet). At the end of the Academic year, the filing can be achieved in the normal way.

A101 and equivalent forms - These details have to be kept secure, in the blue folder in the safe. A copy of all paperwork received with a completed *details form*, held in the front of the folder.

All police enquiries - There is a record sheet in the front of the A101 folder to keep a record of all enquiries from the police. If we don't have an A101 because we have no record of the student and so can't give out any information. Any other enquiries than those released via an A101.
If police come on sight to speak to a student, call CMG Member for Authority so this can happen. Enter info. on the spread sheet in the front of the blue folder in the safe. If the student is under 18 yrs they need to be accompanied by a member of staff, this can be any full time member of staff, often the students tutor will be willing if not a member of CMG.

COLCHESTER INSTITUTE
REQUEST FOR ACCESS TO PERSONAL DATA (STUDENTS

I (insert name)……wish to have access to:

_____

_____

_____

_____

_____

I understand that I will have to pay a fee of £10.

Name (in full): _____

College course attended: _____

Date of Birth: _____

Full Address to which information is to be sent:

_____

_____

_____

_____

_____

Daytime contact telephone number: _____

Student signature: _____

Date: _____

Please return to**:**

Miss Jayne Folkard, Senior Registry Assistant,

Colchester Institute, Sheepen Road, Colchester, Essex. CO3 3LL

For Office use Only:

Request for information received on: _____

Information sent to enquirer on: _____

Signed (Designated Data Controller): _____

Appendix B

Procedure for Police Enquiries/Attendance on Site

Colchester Institute seeks to support its local police in the conduct of their enquiries. However, it must also ensure its duty of care to both learners and employees and must act in accordance with its duty of confidentiality under Data Protection Law. It is important, therefore, that procedures are followed in the event of a police enquiry made to the College and /or when officers attend on site in the course of their duties.

Requests for Information

All enquiries from police officers for information, whether by telephone or letter or other means should be referred in the first instance to:

1. Vice Principal Student Services and Support - in cases involving learners
2. Executive Director Human Resources – in cases involving members of staff
3. The Principal or other College Executive member, in the absence of either of the above
4. The Senior Registry Assistant with responsibility for data release

In instances of requests for personal or detailed information about an individual, the request should be accompanied by a completed A101 form confirming the exact information that is required. A record of information on learners disclosed to the Police will be held by the Senior Registry Assistant with responsibility for data release, and no data will be released without the consent of one of the staff listed in 1, 2 or 3 above.

Whilst each case will be judged on the particular circumstances pertaining, the guiding principle should be to comply with reasonable requests for information within the constraints of Data Protection.

Where Safeguarding information is requested from authorised persons (including the Police; Social Services and Local Safeguarding Children Boards (LSCBs) under a Section 47 of the Children Act 1989 enquiry or where there is “reasonable cause to believe that a child or young person may be suffering or at risk of suffering significant harm,” that information will be shared by a member of the Safeguarding Officers Team. For vulnerable adults the same procedure applies. A record of what information has been shared and with whom will be maintained in the Safeguarding files.

Police Officers Attending on Site

All enquiries from police officers attending on site should be dealt with in accordance with the following procedure:

• Police officer reports to reception, signs in and waits to be collected.
• Reception contact relevant member of staff, as above
• Police officer is collected and accompanied to an interview room. In no circumstances should police officers be invited to move within the site unaccompanied.
• The relevant senior member of staff will establish the reason for Police attendance and instigate appropriate enquires, or seek to provide the relevant information (with completed A101 as necessary)

Should a police officer reasonably wish to see a particular individual, whether learner or member of staff:

- The relevant senior member of staff will make discreet arrangements for the person concerned to be seen by the Police. Efforts should be made to avoid situations where the person concerned is compromised in their work situation. If the person is a learner of 18 years or younger, they should be accompanied by a member of staff at all times.
- In all cases where a learner is under 18 or is classed as vulnerable either because of learning difficulty or disability, the parent/carer will be contacted immediately. Where the parent/carer cannot be contacted then a member of staff will remain with the learner at all times to provide appropriate advocacy.
- Officers attending will be fully briefed by staff on the nature of any disabilities or learning difficulties and, where appropriate, will be assisted in communicating with the learners.
- A full record of all actions taken will be maintained by the senior member of staff present.
- Once the matter is resolved, the police officer should be accompanied in their return to Reception, where they can sign out and leave the site.
- If deemed necessary, security staff should be requested discreetly to support any of the above processes.

Note: These procedures apply in all instances when the Police themselves instigate an enquiry or visit to the college. In circumstances when the college itself calls upon the police to attend on site (e.g. in response to an emergency), arrangements must be made to ensure that they are met on arrival and taken to the location of the incident or event requiring their presence.

Notification from the Police about a learner or member of staff
If a learner or member of staff is considered by the Police to pose a risk, due to an arrest or previous criminal conviction, they Police will write to either:

1. Vice Principal Student Services and Support- in cases involving learners
2. Executive Director Human Resources – in cases involving members of staff

- For learners, refer to the Pending Prosecution or Criminal Convictions Policy for Enrolled Students for further action.
- For members of staff, the Executive Director Human Resources will liaise with the relevant line manager / member of College Management Group to make a decision based on a risk assessment basis. A referral may be made to the Local Area Designated Officer (LADO) if the member of staff may be considered a risk to others, including learners or other staff, the decision whether or not to refer will be made jointly by the Vice Principal Student Services and Support and the Executive Director Human Resources
- Records of all cases relating to staff members, including LADO referrals, will be retained by the Executive Director Human Resources.