Data Protection Policy

Including Records Management, Information Security and Subject Access Request

Issue Date: 25.02.2023

1. Introduction

ELATT collects and uses personal information about staff, pupils, parents, alumnae and other individuals who come into contact with the ELATT. This information is gathered in order to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect, use and disclose information to ensure that ELATT complies with its statutory obligations.

ELATT is registered as a Data Controller on the Data Protection Register held by the Information Commissioner:
Registration Number: Z4684900 (https://ico.org.uk/ESDWebPages/Entry/Z4684900)

Further Education Providers also have a duty to issue a Privacy Notice to all pupils/parents and staff; this summarises the information held, why it is held and the other parties to whom it may be passed on. This is available on ELATT's website and Application Forms.

2. Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulation (GDPR), and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. The policy will be communicated to all staff and they will be expected to understand and abide by it.

3. What is Personal Information?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Examples of personal data are:
a. Name
b. Address
c. Dates of Birth
d. Unique Learner Number
e. National Insurance Number
f. Learning support information

4. Data Protection Principles

The General Data Protection Regulation establishes six enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully;
2. Personal data shall be obtained only for specified and lawful purposes;
3. Personal data shall be adequate, relevant and not excessive;
4. Personal data shall be accurate and where necessary, kept up to date;
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes;
6. Personal data shall be kept secure

5. Definitions

- **"processing"** means obtaining, recording or holding the information or data or carrying out any or set of operations on the information or data.
- **"personal data"** means data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
- **"parent"** has the meaning given in the Education act 1996, and includes any person having parental responsibility or care of a child (ELATT's 16 – 18 year olds).

6. How ELATT will abide by the Act

ELATT is committed to maintaining the above principles at all times. Therefore, ELATT will:

- Process personal information only where it is strictly necessary for legitimate Further Education Providers purposes.
- Collect only the minimum personal information required for those purposes.
- Provide clear information to individuals about how their personal information will be used and by whom.
- Only process relevant and adequate personal information.
- Process personal information fairly and lawfully.
- Maintain an inventory of the categories of personal information processed by ELATT.
- Keep personal information accurate and, where necessary, up-to-date.
- Retain personal information only for as long as is necessary for legal or regulatory reasons or legitimate Further Education Providers purposes.
- Respect individuals' rights in relation to their personal information, including their rights of subject access.
- Keep all personal information, in whatever format, secure.
- Only transfer personal information outside the EEA in circumstances where it can be adequately protected.
- Only apply the exemptions applicable under information legislation.
- Have a regular review and audit of the way personal information is held, managed and used and ensure methods of handling personal information are regularly assessed and evaluated.
- Treat people justly and fairly whatever their age, faith, religion and beliefs, disability, gender, sexual orientation or ethnicity when dealing with requests for information.
- Have clear procedures for responding to requests for information.
- Acknowledge, investigate and fully respond to all complaints relating to a request for information according to the complaints process.

7. Responsibility and Accountability for Data Protection

All staff are responsible for:

- Checking that any information that they provide to ELATT in connection with their employment is accurate and up to date;
- Informing ELATT of any changes to information which they have provided, e.g. change of address;
- On a quarterly basis, checking that all information regarding continuing professional development (trainings completed, qualifications achieved etc.) is fully up to date. This information is occasionally sent to funders for application or reporting purposes.
- Informing ELATT of any errors or changes. ELATT cannot be held responsible for any errors unless the staff member has informed ELATT in writing.
- If, and when, as part of their responsibilities, staff collect information about other people (e.g. about students' course work, opinions about ability, references to other educational establishments, details of personal circumstances), they must comply with the guidelines for staff which are in the Appendices below.

All staff have an individual responsibility to ensure that they comply fully with the GDPR. It is a criminal offence to knowingly or recklessly obtain or disclose personal data **without the consent of the data controller**. Staff should not process any personal data unless they are sure that they are authorised to do so. Staff failing to comply with this policy could be subject to action under the ELATT's disciplinary procedure. The Data Controller's actions are monitored by the CEO and the CEO is monitored by the Trustees to ensure that they all responsible parties are fulfilling their GDPR obligations.

When handling personal information on ELATT's business, trustees must comply with this policy and be aware of their responsibilities as individuals under the GDPR. Trustees should be mindful that it can be a criminal offence to process personal data in a manner which they know that they are not authorised to do.

The **Data Protection Officer (Mia Wylie), ELATT Trustees and Chief Executive of ELATT (Anthony Harmer)** have overall responsibility for ensuring that ELATT:

- Manages its information and records properly and is compliant with all the relevant legislation.
- Complies with this policy;
- Approves procedures where personal information is processed such as:
    - the management and communication of privacy notices;
    - handling of requests from individuals;
    - the collection and handling of personal information;
    - complaints handling;
    - management of personal information security incidents; and
    - outsourcing and off-shoring of personal information processing.

The ELATT management will manage and address the risks to the information and will understand:

- What information is held, for how long and what purpose
- Who has access to protected data and why

8. Data Processing

Personal Data Held

Staff will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

- Personal information about members of the ELATT's community - including students, members of staff, alumni and parents/carers: names, addresses, contact details, legal guardianship contact details, health records, disciplinary records, roll/Unique Learner numbers, nominated next of kin contact details
- Curricular data; class lists, attendance sheets, student progress records and reports.
- Professional records; employment history, taxation and national insurance records, appraisal records and references.
- Any other information that might be disclosed by parents/carers or by other agencies working with families or staff members.

Security of Personal Data

The need to ensure that data is kept securely means that precautions must be taken against physical loss or damage, and that both access and disclosure must be restricted. All staff are responsible for ensuring that:

- any personal data which they hold is kept securely; and
- personal information is not disclosed either orally, in writing, electronically or otherwise to any unauthorised person.

Personal information should be, if hard copy:

- not left accessible to unauthorised persons;
- kept in a locked filing cabinet or in a locked drawer. If secure storage is not available in community delivery venues, personal information will be stored at ELATT; and
- disposed of as confidential waste.

If electronic:

- password protected
- held on a PC with 'time out' facility and/or Pro Suite MIS system.
- deleted in accordance with retention contractual periods
- network passwords to be enforced through strong passwords and a termly prompt to change passwords

Every electronic system that holds personal information has a designated manager who has overall responsible for controlling access to and the information security of that system, this being the ELATTs IT Services Coordinator (Orla Donnelly). Advice on making personal data secure is provided by the Data Protection Officer (DPO) (Mia Wylie).

Any incidents where personal data has been lost or disclosed to unauthorised recipients must be immediately reported to the Data Protection Officer (Mia Wylie) and Chief Executive of ELATT (Anthony Harmer) who will advise what action should be taken to mitigate the damage. ELATT must inform the Information Commissioners Office (ICO) within 72 hours of becoming aware that a data breach has occurred. Those affected will be notified without undue delay.

External Data Processing

All contracts with third-party providers, where the processing of personal data is required, shall include a requirement for the contractor to comply with the requirements of the General Data Protection Regulation. This includes ELATT's external contractors, MIS Systems (Pro-Suite, Pro-achieve, Awarding Bodies etc.), all email & IT service providers and ELATT's cleaning and caretaking companies, if any.

Special Category and High Risk Personal Data

Special category personal data is defined in the Act as information concerning an individual's:

- racial or ethnic origin
- political opinions
- religious beliefs or other beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life
- criminal convictions or alleged offences
- biometric data

Extra care must be taken when processing special category personal data as additional requirements under the Act must be met to ensure that the processing is legitimate and safe. The advice of the Data Protection Officer should be sought before any new processing of special category personal data commences. There is also some personal information which is regarded as high risk and therefore a risk assessment should be carried out and additional security precautions should be implemented before processing such information. High risk personal information includes, but is not limited to:

- personal bank account and other financial information;
- national identifiers, such as national insurance numbers;
- personal information relating to vulnerable adults and children;
- detailed profiles of individuals;
- sensitive negotiations which could adversely affect individuals; and
- large numbers of records containing personal information.

Medical Records

These are classed as sensitive personal data under the Act and, therefore, additional care should be taken when processing this information. In particular, before disclosing the medical records of anyone as part of a Subject Access Request (SAR), the advice of the relevant medical practitioner and the Data Protection Officer must be sought as to whether the information should be released or not.

Staff Records and the Monitoring of Staff

ELATT will comply with the Information Commissioner's (ICO's) employment practices code in relation to the processing of staff personal information. This Code exemplifies good practice and strikes a balance between the legitimate expectations of workers that personal information about them will be handled properly and the legitimate interests of employers in deciding how best, within the law, to run their own businesses. In particular, staff monitoring should only be carried out in accordance with this code of practice.

Recording of Telephone Calls

Individuals must be informed at the beginning of any call if the telephone call is being recorded in any format. Currently ELATT does not record phone calls. Should this happen, the individual must be advised what information is being recorded, the reasons for recording the information, whether the information will be shared with anyone else and, if so, whom it will be shared with and for how long the information will be retained.

Publication of Personal Data

Personal data should generally only be made public if there is a legal or statutory requirement to do so. On occasion it may be appropriate to publish personal information with the individual's consent. However, in such cases staff must ensure that the consent is fully informed and freely given. Staff must also be aware that it is possible to withdraw consent at any time and, if that happens, publication of the data must cease immediately. Staff need to be aware that publishing personal information on ELATT's web pages or internet effectively means that the information is published world-wide and outside the European Economic Area (EEA). It, therefore, cannot be protected by the GDPR or the European Directive on Personal Privacy. Great care must be taken before publishing personal information (or any information from which individuals could be identified) in this manner and the approval of the CEO should be obtained before publication of information.

In some cases, a funder will require employees' personal data. These may be current personal address, qualification details, DBS number and/or record, date of birth, payroll number, details of expenses, job title or working hours. This may be as part of the vetting process for grant applications (e.g. Big Lottery Fund and others), as an anti-fraud measure (e.g. AMIF, ESF grants, and others) or for safeguarding purposes (e.g. lead contractors such as, but not limited to, Local Authorities and FE Colleges).

Retention and Disposal of Data

It is the responsibility of the individual service areas holding personal information to ensure that the information that they hold is kept accurate and up-to-date and is not held for any longer than is necessary for the purpose for which it was collected. When the data is no longer required ELATT must dispose of the data safely. Staff files must be kept for 6 years (unless otherwise specified) following contract termination and student files, in the case of students under 18, until the student is 25 years old, and adult students according to the rules of the particular funder (e.g. European Social Fund and other European funding sources require retention of data for up to 13 years in some cases – see Document Retention and Archiving Policy). Data is held securely both on and offsite. Further advice and information is available from the Information Commissioner's Office, https://ico.org.uk/global/contact-us/

Records Management

ELATT recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to its effective overall management. Records provide evidence for protecting the legal rights and interests of ELATT and provide evidence for demonstrating performance and accountability.

Records are defined as all those documents which facilitate the business carried out by ELATT and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

ELATT has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The persons with overall responsibility for records management are the CEO and DPO. They will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. ELATT will also monitor compliance with this policy by surveying at least annually to check if records are stored securely and can be accessed appropriately.

All staff must ensure that records for which they are responsible are accurate and are maintained and disposed of in accordance with ELATT's records management guidelines and Document Retention and Archiving Policy.

9. Access to Data and Disclosure

Data Subjects Rights

ELATT will 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 right of access to one's personal information;
- the right to prevent processing in certain circumstances; and
- the right to correct, rectify, block or erase information which is regarded as wrong information.
- the right to ask us to erase your personal information in certain circumstances
- the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.
- the right to ask us for copies of your personal information.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Subject Access

Any individual who wants access to their personal data, must write to the DPO with their request (via post, or email to hello@elatt.org.uk or mia@elatt.org.uk). The data will be issued within one calendar month (or 15 working days for information in a student's educational record). If there is any doubt about whether it is permissible to release particular information, the CEO/DPO will take the recommended view that it is better not to release the information as it can always be released at a later date with little harm, whereas if released in error it cannot easily be recovered.

Subject Consent

Staff must ensure that any consent given for the processing of personal information is fully informed and freely given, that individuals are aware that they may withdraw consent at any time and what the consequences are if they withdraw their consent. ELATT's learning community includes people with ESOL needs and/or additional learning needs such as learning difficulties and visual and hearing impairments. It is our policy to make all necessary accommodations to ensure that these learners are able to give fully informed consent. Our student handbook, which is written in an ESOL accessible style, contains a summary of our data protection policy and privacy notice. Consent forms are expressed in accessible language. When seeking the consent of a learner with additional learning needs, their course tutor will provide the support required, including translation, large print, reading aloud or other necessary accommodations.

If it is deemed that the consent of individuals is necessary, staff need to be aware that, in the case of special category personal data, individuals have to give explicit consent to the processing. It is ELATT's good practice to obtain written consent in such cases.

External Disclosure Requests

Requests from external organisations or third parties for personal information about individuals should be passed to the CEO/DPO (who may consult advisers). Under no circumstances should any personal information about any individual be passed outside ELATT without the authority of the CEO/DPO. All requests must be put in writing to the CEO/DPO.

10. Sharing Information

Within Further Education Providers

Before sharing personal information internally, it is the responsibility of individual members of staff to ensure that they have the authority to do so and that the recipient is authorised to receive such information. Failure to do so could lead to action under ELATT's disciplinary procedure (and, in

exceptional circumstances, criminal charges). If there is any doubt, individuals should seek the advice of the CEO/DPO. Personal information must be sent only to relevant subject and pastoral staff.

Externally

There are occasional instances where information is shared with partners or outside organisations, such as those companies that support with MIS or achievement software. Sharing will occur where a written contract for service is in place (which sets out the third parties responsibilities to comply with GDPR), where ELATT has a statutory responsibility to share information or for the protection of students in line with ELATT's Safeguarding Policy. Sharing takes place via the partner's secure portal (for example a Dropbox folder accessed via a private, time-limited link) and the partner is required to complete a bespoke data protection agreement specifying the length of time they can keep the data and for what purpose. Further details are contained within the relevant ELATT's Privacy Notice, available from ELATT's website.

11. Complaints

Where relevant, complaints will be dealt with in accordance with ELATT's Complaints Policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

12. Status of the Policy

All staff must adhere to this policy. Any failure to follow the policy can result in disciplinary proceedings. Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct in some cases.

Any member of staff who considers that the policy has not been followed should raise the matter with the CEO/DPO, or the Chair of Governors if it concerns the CEO.

13. Contacts

If you have any queries or concerns regarding this policy/procedure then please contact the Data Protection Officer:
Mia Wylie, mia@elatt.org.uk

Or write to the address below:
ELATT, 260 Kingsland Road, London, E8 4DG

14. Review

This policy will be reviewed annually. It was last updated in February 2022.

Appendix: Data Breach Procedure

ELATT holds large amounts of personal and sensitive data. Every care is taken to protect personal data and to avoid a data protection breach. In the event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This procedure applies to all personal and sensitive data held by ELATT and all ELATTs staff, trustees, volunteers and contractors, referred to herein after as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at ELATT if a data protection breach takes place.

Legal Context

Article 33 of the General Data Protection Regulations: Notification of a personal data breach to the supervisory authority:

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance.

Types of Breach

Data protection breaches could be caused by a number of factors. A number of examples are shown below:

- Loss or theft of student, staff or governing body data and/ or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Poor data destruction procedures;
- Human error;
- Cyber-attack;
- Hacking.

Managing a Data Breach

In the event that ELATT identifies or is notified of a personal data breach, the following steps should be followed:

1. The person who discovers/receives a report of a breach must inform the CEO/DPO or, in her /his absence, management of ELATT. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable.
2. The CEO/DPO (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT technician.
3. The CEO/DPO (or nominated representative) must inform the Chair of Governors as soon as possible. As a registered Data Controller, it is the ELATT's responsibility to take the appropriate action and conduct any investigation.
4. The CEO/DPO (or nominated representative) must also consider whether the Police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future. In such instances, advice from the ELATT's legal support should be obtained.
5. The CEO/DPO (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
    a. Attempting to recover lost equipment.
    b. Contacting the relevant Council Departments, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned. Consideration should be given to a global email to all staff. If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details if possible and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the CEO/DPO (or nominated representative).
    c. The use of back-ups to restore lost/damaged/stolen data.
    d. If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.
    e. If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

Investigation

In most cases, the next stage would be for the CEO/DPO (or nominated representative) to fully investigate the breach. The CEO/DPO (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- The type of data;
- Its sensitivity;
- What protections were in place (e.g. encryption);
- What has happened to the data;
- Whether the data could be put to any illegal or inappropriate use;
- How many people are affected;
- What type of people have been affected (students, staff members, suppliers, etc) and whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it. The investigation should be completed as a matter of urgency due to the requirements to report notifiable personal data breaches to the Information Commissioner's Office. A more detailed review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

Notification

Some people/agencies may need to be notified as part of the initial containment. However, the decision will normally be made once an initial investigation has taken place. The CEO /DPO (or nominated representative) should, after seeking expert or legal advice, decide whether anyone is notified of the breach. In the case of significant breaches, the Information Commissioner's Office (ICO) must be notified within 72 hours of the breach. Every incident should be considered on a case by case basis.

When notifying individuals, give specific and clear advice on what they can do to protect themselves and what ELATT is able to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the ELATT's Complaints Procedure). The notification should include a description of how and when the breach occurred and what data was involved. Include details of what you have already done to mitigate the risks posed by the breach

Review and Evaluation

Once the initial aftermath of the breach is over, the CEO /DPO (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be reported to the next available Senior Management and Board meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance. This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance.

Implementation

The CEO /DPO will ensure that staff are aware of the ELATT's Data Protection policy and its requirements including this breach procedure. This should be undertaken as part of induction, supervision and ongoing training. If staff have any queries in relation to ELATT's Data Protection policy and associated procedures, they should discuss this with their line manager, DPO or the CEO.

APPENDIX: Staff Guidelines for Data Protection

1. ELATT staff will process information about students on a regular basis, when marking registers or ELATT work, writing reports or references, or as part of a pastoral or academic supervisory role. ELATT 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 Data Protection Act (1998) and GDPR The General Data Protection Regulation (GDPR) (EU) 2016/679).

The information that staff deal with on a day-today 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;
- Notes of personal supervision, including matters about behavior discipline.

2. Information about a student's physical or mental health; sexual life; political or religious views; trade union membership or ethnicity or race is sensitive and can only be collected and processed with the student's consent.

3. All staff have a duty to make sure that they comply with the data protection principles which are set out in ELATT 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 College policy

4. ELATT will designate staff as 'authorised staff'. These are the only staff authorised to hold or process data that is:

- Not standard data or
- Sensitive data

'Authorised staff' are:

- The lead tutor, tutor and keyworker
- The MIS manager and MIS officer
- The Student Support Coordinator
- IT Services Coordinator and Technician
- The Fundraising Team

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

- in the best interests of the student or staff member, or a third party, or the
- ELATT 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 the circumstances

This should only happen in very limited circumstances.

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

6. Staff must not disclose personal information to any student, unless for normal academic or pastoral purposes, without authorisation or agreement or in line with ELATT policy.

7. Staff should not disclose personal information to any other staff member except with authorisation or in line with ELATT policy.

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

Staff Checklist for Recording Information

- Do you really need to record the information?
- Is the information “standard” or is it “sensitive”?
- If it is “sensitive”, do you have the individual’s express consent?
- Has the student been told that this type of information will be processed?
- Are you authorised to collect/store/process the data?
- If yes, have you checked with the individual that the data is accurate?
- Are you sure that the information is secure?
- If you do not have the individual’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 information?
- Have you reported the fact of information collection to the authorised person within the required time?

APPENDIX 2
Standard Request form for access to Information

I, _____,wish to have access to either:

1. All the information that ELATT currently has about me, either as part of an automated system, or part of a relevant filing system

   Or;

2. Information that ELATT has about me in the following categories (please tick):

- Academic marks or course work details
- Academic or employment references
- Disciplinary records
- Health and Medical matters
- Political, religious or trade union information
- Any statements of opinion about my abilities or performance
- Personal details including name, address, date of birth etc
- Other information, please list below:

Print Name:

Signed:

Date: