



Lancashire

Global Education Centre

Data Protection

Section A: Policy Statement

Section B: General Guidelines

Section C: System Management Procedures

*LGEC is registered as Lancashire Development Education Group Ltd.
Company Limited by Guarantee No. 04244912
Registered Charity No. 1089036*

Data Protection Act 1998

Section A:

This is the Data Protection Policy Statement of **Lancashire Global Education Centre** at 37, St. Peter's Square, Preston, Lancs, PR1 7BX

Our statement of general policy is:

- To comply fully with the Data Protection Act 1998.
- To recognise the right of individuals to have their personal information respected and properly maintained.
- To ensure that anyone acting on LGEC's behalf complies with the Act and does not breach any part of it.
- To provide appropriate guidance on responsibilities under the Act, and training if required, to staff, trustees and, where relevant, volunteers.
- To draw up and implement appropriate management procedures for each set of relevant records, using the appended Guidelines.
- To empower the Chair of Trustees to monitor our compliance with the Act
- To implement disciplinary procedures for misuse of personal data
- To review and revise this policy as necessary, at least annually.

Section B

Guidelines: Data Protection

1: Introduction

The Data Protection Act 1998 relates to **Personal data**. This is information about living, identifiable individuals. This need not be particularly sensitive information and can be as little as a name and address.

Personal = data referring to identifiable, living individuals. Therefore if the information that we keep would allow anyone to identify someone then it is personal. This need not be particularly sensitive information and can be as little as a name and address. It also includes photographs.

Data =

- information held on computer (this however is broader than a pc – it can refer to anything automated i.e. electronic diaries, palm tops, microfiche etc.),
- information in relevant manual files, (card indexes, personnel files etc.)
- information intended to become part of one of the above systems (e.g. proforma's for gathering info going on a database, etc.)

The Data Protection Act works in two ways, by

- **giving individuals** (data subjects) **certain rights**. The data subject is anyone whose personal data is processed. This can however be split up into 'primary data subject' and 'secondary data subject'.

Primary data subject = the person to whom the data refers

Secondary data subject = data about people related to the primary data subject e.g. next of kin – if they can easily be identified from the data.

- **requiring those who record and use personal information** (data controllers) to be open about their use of that information and to follow sound and proper practices (the Data Protection Principles).

The Data Controller can be any type of company, organisation or individual, and need not necessarily own a computer. The size of the organisation is immaterial; the nature of the organisation is unimportant; the amount of personal data held is irrelevant. LGEC is a data controller. The Chair of Trustees will monitor compliance with the Act on behalf of LGEC.

LGEC must comply with the eight Data Protection Principles. The onus is on LGEC, the data controller, to ensure that use of data by staff, trustees, volunteers or contractors does not breach the eight Data Protection Principles.

1a Data Protection Principles

Data must be:

- i) obtained fairly and lawfully
- ii) held only for specific and lawful purposes and not processed in any matter incompatible with those purposes
- iii) relevant, adequate and not excessive for those purposes

- iv) accurate and where necessary kept up to date
- v) not kept for longer than necessary
- vi) data should be processed in accordance with the rights of data subjects under the Act. This includes having the right to:
 - Be informed upon request of all the information held about them by a particular data controller
 - Prevent the processing of their data for the purposes of direct marketing
 - Compensation if they can show that they have been caused damage by any contravention of the Act
 - The removal or correction of any inaccurate data about them.
- vii) Adequate security precautions must be in place to prevent the loss, destruction or unauthorised disclosure of the data.
- viii) Data must not be transferred outside the European Economic Area unless you are satisfied that the country in question can provide an adequate level of security for that data. However, you may always transfer data outside the EEA where you have the subject's consent.

1b Definitions under the Data Protection Act

Fair processing: when you collect information from individuals you should be honest and open about why you want it. In addition, you must have a legitimate reason for processing the data. You should explain (in most cases in writing):

- Who the data controller is (LGEC)
- What you intend to use the information for
- To whom you intend to give the personal data. This may be a specific third party, or may be a more general description such as 'other companies', 'suppliers' etc.

If you use, or intend to use, personal data for direct marketing purposes, you should ensure that data subjects are made aware of this and given an opportunity not to have their particular data processed for this purpose.

Adequate, relevant and not excessive: data users (LGEC staff/trustees/volunteers) should monitor the quantities of data held for their purposes and ensure that they hold neither too much nor too little data in respect of the individuals about whom their data is held. You must only hold the data ***which you actually need***.

Accurate: personal data should be accurate and any errors must be corrected.

No longer than necessary: only in exceptional circumstances should data be kept indefinitely. You should have a system for the removal of different categories of data from your system after certain periods.

Security: adequate security must be provided for the data, taking into account the nature of the data, and the harm to the data subject which could arise from disclosure or loss of data.

Authorised access to computer records: only people who are authorised can gain access to personal data. Written procedures are attached setting out who is authorised to access which records and for what purpose. Misuse of personal data by members of staff will be a disciplinary offence.

Access to records by individuals other than staff: Particular attention should be given to:

- a) the siting of computer terminals so as to prevent casual callers to premises being able to read personal data on screen (this is particularly important in the case of the resources centre computer). Care should also be taken when using laptop computers out of the office.
- b) Procedures to verify the identify of callers (especially telephone callers) seeking information held on computer.

Prevention of the accidental loss or theft of personal data: Attention must be given to unforeseen contingencies such as the theft of computer equipment or fire. Consideration should be given to:

- a) Keeping back-up copies of files in secure areas away from the computer on which they are normally used
- b) The physical security of computer equipment

Sensitive Data

There are eight categories of sensitive personal data:

- 1 the racial or ethnic origin of data subjects
- 2 their political opinions
- 3 their religious beliefs or other beliefs of a similar nature
- 4 membership of trade unions
- 5 physical health, mental health or condition
- 6 their sexual life
- 7 the commission or alleged commission of any offence
- 8 any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court of such proceedings

If **any** such information is held, it is likely that you will need the explicit consent of the individual concerned and security procedures will have to be adequate for the protection of sensitive data.

Manual Data: Such records need not be notified to the Commissioner, but should be handled in accordance with data protection principles. Manual records are covered by the Act if they form part of any relevant filing system defined as “*any set of information relating to individuals and structured, either by reference to criteria relating to individuals, or in such a way that specific information relating to a particular individual is readily accessible*”. (ie If you can search the records for information on an individual, the system is a relevant one.)

Compensation: individuals may seek compensation through the courts if they have suffered damage because of any contravention of the Act.

Subject access requests: must be dealt with promptly and certainly within 40 days of the date of receipt. LGEC will legitimately ask for a fee of £10 and the 40 day period will not begin until this is received. In response to a request, individuals are entitled to a copy of the information held about them, both on computer and as part of a relevant filing system. They also have the right to receive a description of why their information is processed, anyone it may be disclosed to, and any information available about the source of the data.

It is important that staff know how to recognise a subject access request and realise that it must be dealt with urgently.

Dealing with direct marketing suppression requests: individuals have the right not to have their personal data processed for direct marketing purposes. When collecting data, you should give people the opportunity to let you know whether or not they wish to receive marketing material from you. If they do not, or if you do not ask this question, you must ensure that you can suppress their details on any mailing lists you use. If it is intended to share information for direct marketing purposes you must first check with the individuals concerned if they are happy for you to do this. This should be done when you first collect the data, perhaps on an application form. You must not pass on the details of anyone who says that they object to their details being used in this way. If you have not previously sent out marketing material or passed on details to third parties for marketing, you should obtain the consent of existing customers before beginning to process their data for these purposes.

1c What Sort of Records?

In LGEC's case, the sort of records we hold include:

- *Membership details*
- *Personnel records*
- *Recruitment records*
- *Volunteer records*
- *Booking details for training events*
- *Photographs*
- *Emails - please note emails are often legally equivalent to paper documents and therefore information about living, identifiable individuals included is constituted as personal data*

All staff must consider whether information they hold (paper or electronic) falls within the definition of the Act and draw up appropriate guidelines for inclusion in this Policy (see Section C).

1d Record Keeping and Disposal

Introduction

Only those documents should be retained that are relevant, accurate, up-to-date and essential to meet their purpose. When they become out of date and of no further use, they should be removed and destroyed (shredded). It is good practice to set retention periods on all documents. LGEC's manual personnel and payroll records will be kept in a locked filing cabinet, with keys held by the Chief Executive and other authorised staff (Finance Manager and Projects Manager). Personnel information held on computer (such as letters) will have secure password protected access and deleted once their immediate use has passed and a paper copy (where required) has been filed. LGEC's computer hard drives must be wiped before disposal of the computers. Work done on home computers should be stored on disks which will be destroyed at the end of their life.

References

Confidential employment references *given by* LGEC are exempt from the right of access provisions of the Act. For practical reasons, it is sensible not to keep copies of such references in the employee's file.

References *received by* LGEC are not exempt, provided that the identity of a third party is not divulged without permission (eg the author). The spirit of the Act is about openness and the Guidance from the Data Commissioner is that, if possible, a copy of the reference should be provided but with information about third parties removed if it is not practical to gain their consent. In future, when requesting references, LGEC could consider whether to inform referees that the subject of the reference will be entitled to have access to it.

Both successful and unsuccessful job applicants also have the right of access to application forms, interview notes, test results etc, retained in a recruitment file by the employer or by the recruitment agency. In principle, the records should be destroyed once the purpose for keeping them no longer exists, ie when all the decisions have been taken and the campaign is over. However, this must be balanced against the possible need to defend the decisions against a claim of discrimination.

Disposal

The Data Protection Act 1998 places an obligation on LGEC to dispose of personal information when it is no longer needed. To prevent unauthorised or accidental disclosure of the information, it is important to exercise care in its disposal, including protecting its security and confidentiality during storage, transportation, handling and destruction. All staff have a responsibility to consider safety and security when disposing of personal information in the course of their work – such information should be shredded if on paper and permanently deleted from computer hard drives.

The ensuing chart summarises the legal requirements associated with certain kinds of information. When deciding on retention times, consider the following **in order**:

- i) any legal requirements (eg possible negligence action);
- ii) The length of any appeals procedure relating to the information
- iii) The number of times in the last two or three years that you have had to refer to a particular type of record (if the answer is never, then get rid of it)

Disposal records should be kept, indicating what records have been destroyed, when, by whom, and using what method of destruction. Records which have been kept or archived may also be tracked. The record may consist of a simple list on paper or be part of an electronic records management system; The disposal record applies to both paper and electronic records. It must not, in itself, contain personal information (eg names). It should include the date and manner of disposal.

Section C: System Management Procedures

1. Membership

- i) Our application forms, and renewal forms, will give an indication of the purposes for which the information may be used. We need to consider whether we will be undertaking direct marketing to our members and if so, make further amendments to the wording below.

The following wording will be added to our membership forms and renewal letters:

- *“Details provided on this form will be used for processing LGEC’s membership scheme and to enable our staff and volunteers to make contact with you in connection with the work we undertake. Members will receive information from LGEC relating to our work and to the work of organisations working in related fields. Please tick this box if you do not wish your details to be given to other organisations working in related fields.”*
- ii) The computer database of members should record the above consent.
- iii) We must ensure, when giving out information, that the enquirer is who they say they are and be satisfied that they are *representing ‘an organisation working in a related field’* and that they will not be using the information for marketing.
- iv) All members (not just those who pay) should be given the annual chance to opt in to receiving our information. This must be done affirmatively (ie we cannot assume that no response means that they wish the status quo to continue). Computer records should show when this response was last obtained.
- v) Two renewal notices will be sent out over a four-month period. If no response is obtained within that time the membership will lapse and the computer record will be deleted.
- vi) The membership database must be password protected and only authorised personnel should have access.
- vii) Manual records printed out from the database must be kept in a confidential environment (eg not left on desks or displayed on noticeboards). Such records may only be supplied to authorised users and must be updated monthly. Any interim changes of information (eg change of address or notification of death) must be amended on the manual lists. Out of date manual lists should be shredded.
- viii) A back up of the membership database must be made monthly and stored out of the office.
- ix) On disposal of the computer on which the database is maintained, action will be taken to ensure that the database is permanently erased from the hard drive.
- x) Archive membership records will be retained for a period of two years and then securely disposed of.

2. Personnel Data

Personnel Records

All employment records shall be filed in the Chief Executive's office in a lockable filing cabinet, accessible by the Chief Executive and other authorised staff (Finance Manager and Projects Manager). The employment record contains details of the employee's job application, references, job description, contract, notes from meetings or any correspondence relating to employment terms and any formal grievance procedures.

A second file containing support and supervision and appraisal records may also be accessed by the employee's line manager. Any information the employee or line manager wishes be confidential, may be stored separately or in a sealed envelope marked with names of people with authorised to read it.

Timesheets, plans and reports are kept in a file open to all staff. If requested, details of sickness absence may be kept in the employment file to protect the employee's privacy. Details of wages payments are stored in a lockable filing cabinet and accessible only to the Chief Executive and the Finance Manager.

Personnel documents are retained according to the table below and shredded at the end of this period.

A list of LGEC employee's personal contact details is distributed to all employees and should not be displayed in the centre where visitors or a member of the public could view it. **Do not** pass on a staff member's personal contact details to anyone outside LGEC without the person's consent. The list says which employee has consented for their details to be given out.

Employment Issues

If confidentiality is an issue for an employee, this should be discussed and agreed with the Chief Executive or Chair of Trustees and the employee. Matters that significantly affect work may need to be discussed with the Management Committee. No one should be told more than they need to know in order to deal with work-related effects of the situation. Any personal matters that do not directly affect work must be treated in absolute confidence and the greatest discretion should be used in disclosing those matters that do not affect work. No one should agree to confidentiality before the person says what it is they want kept secret.

Recruitment

Access to job applications is restricted to the interviewing panel and the administrator overseeing the recruitment process. Equal Opportunities monitoring forms are separated from applications on receipt and all selection scoring sheets are kept for at least 6 months after an appointment before being destroyed.

During recruitment, documents related to applicants are filed securely and access is limited to the interview and selection panels and authorised administration staff. Applicants are requested to send their applications to a named person and to mark their application forms 'confidential'. At the end of the recruitment process copies of all documents are returned to the administrator for filing or secure destruction as required.

When obtaining job references, we will ask the referee if they consent to the candidate seeing the reference if they request to do so.

Personnel information held on computer is password protected and removed as soon as the need for its retention is passed.

Type of Data	Retention Period	Reason
Personnel files including training records and notes of disciplinary and grievance hearings	6 years from the end of employment	References and potential litigation
Application forms/interview notes of unsuccessful candidates	At least six months from the date of the interview	Time limits on litigation
Facts relating to less than 20 redundancies	Three years from the date of redundancy	As above
Income Tax and NI returns, including correspondence with the tax office	At least 6 years after the end of the financial year to which the records relate	Income Tax (Employment) Regulations 1993 Charity Law
Statutory Maternity Pay records and calculations	As above	Statutory Maternity Pay (General) regulations 1986
Statutory Sick Pay records and calculations	As above	Statutory Sick Pay (general) Regulations 1982
Wages and salary records	Six years	Taxes Management Act 1970
Accident books; records and reports of injuries and diseases	At least three years after the date of the last entry	Social Security (Claims and Payments) Regulations 1979 RIDDOR 1995
Health records	During employment	Management of Health and Safety at Work Regulations
Health records where reason for termination of employment is connected with health, including stress-related illness	Three years after termination of employment	Limitation period for personal injury claims
Medical records kept by reason of the Control of Substances Hazardous to Health Regulations 1999	40 years	COSHH Regulations 1999

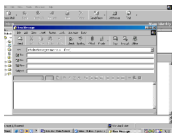
3. Other Information

Meetings

If an item is considered confidential the chair should state this clearly and ensure everyone at the meeting is aware the item is confidential and what this means. Notes should always be taken and kept in an appropriate place. In some cases this will be with the chair and not included in the circulated minutes.

E-mails

All e-mail addresses should have consent from the individual to be kept in an address book, therefore if someone sends you an e-mail it is ok to assume they intend you to keep it. To avoid inadvertently passing it on to other people, all group e-mails should be entered into the **BCC:** address box, as this doesn't display e-mail addresses to the recipients. Clicking on **View** then



All Headers when you create a New Message can show this

function.

Messages

Telephone message pads have a carbon copy of all messages recorded, therefore should not be left where visitors or a member of the public could view them. Old pads will be kept in a secure place and destroyed a month after the last entry.

Authorisation for viewing and using of information

Type of information	Who is authorised to view and use
Membership details	All LGEC Staff members
Personnel records	Chair of trustees, Chief Executive, Finance Manager and Projects Manager
Recruitment records	As above
Volunteer records	As above plus relevant project workers where appropriate
Booking details for training events	Relevant project workers and authorised admin staff where appropriate
Emails	All LGEC staff are responsible for their own email correspondence in accordance with the act
Photographs	As above

Last amended: February 2008 with changes to reflect organisational structure.