

Link School of English Data Protection Policy

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, 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. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines [Link School of English](#) collects and uses personal information about staff, students and other individuals who come into contact with the school. This information is gathered in order to enable it to provide [educational service](#) and other associated purposes. In addition, there may be a legal requirement to collect and use information to ensure that the school complies with its statutory obligations.

What is Personal Data?

[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 that school holds include: students registration forms, emails between staff related to a student, human resources files.

Data Protection Principles

[The Data Protection Act 1998](#) sets out eight 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 one or more specified and lawful purpose
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 processed in accordance with the rights of data subjects under the Data Protection Act 1998;
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security;
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Data Types

Personal data is defined by the Act as data which relates to a living individual who can be identified from that data or from that data and other information which is in the

possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

The Act also defines “sensitive personal data” as personal data relating to the racial or ethnic origin of the data subject; their political opinions; their religious (or similar) beliefs; their physical or mental health condition; their sexual life; the commission or alleged commission by them of any offence; or 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 in such proceedings.

At least one of the following conditions must be met whenever Link School processes personal data:

- the individual to whom the personal data refers has consented to the processing.
- the processing is necessary in relation to a contract which the individual has entered into or because the individual has asked for something to be done so they can enter into a contract
- the processing is necessary because of a statutory obligation that applies to an individual
- the processing is necessary to protect the individual’s “vital interests”; this condition only applies in cases of life or death, such as where an individual’s medical history is disclosed to a hospital’s A&E department treating them after a serious road accident
- the processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions.

In addition to the conditions described above, at least one of the following conditions must also be met whenever Link School processes sensitive personal data:

- the individual who the sensitive personal data refers to has given explicit consent to the processing
- the processing is necessary to comply with employment law
- the processing is necessary to protect the vital interests of the individual (in a case where the individual’s consent cannot be given or reasonably obtained) or another person (in a case where the individual’s consent has been unreasonably withheld)
- the processing is carried out by a not-for-profit organisation and does not involve disclosing personal data to a third party, unless the individual consents
- the individual has deliberately made the information public
- the processing is necessary in relation to legal proceedings; for obtaining legal advice; or otherwise for establishing, exercising or defending legal rights
- the processing is necessary for administering justice, or for exercising statutory or governmental functions
- the processing is necessary for medical purposes, and is undertaken by a health professional or by someone who is subject to an equivalent duty of confidentiality

confidentiality

the processing is necessary for monitoring equality of opportunity, and is carried out with appropriate safeguards for the right of individuals.

Access to personal data by Data Subjects

The DPA provides individuals with a right to request access to the personal data that an organization holds for them. This right enables individuals to understand how their personal information is used, to check the accuracy of the information and exercise their right over processing of that information.

A Data Subject may make a subject access request (“SAR”) at any time to see the information which Link School holds about them. A valid request must:

- be for that individual's personal data
- be made in writing (email is accepted)
- include the appropriate fee (Link school currently requires a fee of £30)

Upon receipt of a SAR Link School shall have a maximum period of 40 working days within which to respond. The following information will be provided to the data subject:

- a description of any personal data held on the data subject
- details of what that personal data is used for
- details of any third-party organisations that personal data is passed to

Third party access

A data subject may authorise any other person (e.g a relative) to make a subject access request on their behalf. In most cases written authority from the data subject should be provided before the school can comply with the request.

Data security policy

Link School collectively, and its staff and students individually, are responsible for ensuring that appropriate technical and organisational measures are taken against the unauthorised or unlawful processing of personal data as well as against accidental loss or destruction of, or damage to, personal data.

Procedure

Link School staff and students must ensure that they employ safeguards for personal data that is proportional to the risks presented in their processing activities. Any staff or students who discover a potential or actual security breach must immediately inform the Managing Director.