Data Protection Policy

Reviewed and updated 01.09.2025

This document is a statement of the aims and principles of the School, for ensuring the confidentiality of sensitive information relating to staff, pupils, parents and governors.

Introduction

L'école bilingue needs to keep certain information about its employees, pupils and other users to allow it to monitor performance, achievements, and health and safety, for example. It is also necessary to process information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government complied with.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, l'école bilingue must comply with the Data Protection Principles which are set out in the Data Protection Act 2018, alongside the UK General Data Protection Regulation (UK GDPR).

The key principles of the General Data Protection Regulation (GDPR):

1.1 **Lawfulness, fairness and transparency**- Transparency: Tell the subject what data processing will be done. Fair: What is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)].

1.2 **Purpose limitations** - Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.

1.3. **Data minimisation** - Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. In other words, no more than the minimum amount of data should be kept for specific processing.

1.4. **Accuracy**- Data must be "accurate and where necessary kept up to date" [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Data holders should build rectification processes into data management / archiving activities for subject data.

1.5. **Storage limitations** - Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. In summary, data no longer required should be removed.

1.6. **Integrity and confidentiality**- Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [article 5, clause 1(f)].

1.7. **Accountability** - The accountability principle in Article 5(2) is the GDPR requires the school to demonstrate that they comply with the principles and states explicitly that this the responsibility of the school.

All staff or others who process or use personal information must ensure that they follow these principles at all times. Any failures to follow this policy can result in disciplinary proceedings.

Responsibilities of Staff

● All staff are DBS checked and records are held in one central record on 'Online SCR'.
●All staff are responsible for: Checking that any information that they provide to the school in connection with their employment is accurate and up to date.
●Informing the school of any changes to information that they have provided, e.g. change of address, either at the time of appointment or subsequently. The school cannot be held responsible for any errors unless the staff member has informed the school of such changes. However, once the school has been informed of any change in circumstances, their record must be updated as soon as practicable.

Data Security

All staff are responsible for ensuring that:

● Any personal data that they hold is kept securely through digital encryption or in physical locked storage
● If and when, as part of their responsibilities, staff collect information about other people (e.g. about a student's course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff.
● Personal information is not disclosed either orally or in writing or via digital or by any other means, accidentally or otherwise, to any unauthorised third party.

Personal information should:

● Be stored away safely; or
● If it is computerised, be coded, encrypted or password-protected
● Computer printouts as well as source documents must be shredded before disposal.

Any queries or concerns about security of data in the school should in the first instance be referred to the Headteacher or the Head of Administration. The school is liable in law under the terms of the GDPR, and staff are responsible for ensuring that practices that have been put in place by the school are adhered to. The school may also be subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this General Data Protection Policy by a member of staff will be treated as disciplinary matter, and serious breaches could lead to dismissal.

Authorised disclosures

The School will, in general, only disclose data about individuals with their consent. However, the school is required, by law, to pass on some of this personal data to the local authority and the Department for Education (DfE).

Whilst the majority of pupil information provided to the school is mandatory, some of it is provided to on a voluntary basis. In order to comply with the General Data Protection Regulation, the school will inform parents whether they are required to provide certain pupil information to us or if they have a choice in this.

The categories of pupil information that is collected, held and shared include:
- Personal information (such as name and address)
- Characteristics (such as ethnicity, language, nationality)
- Attendance information (such as sessions attended, number of absences and absence reasons)

Information collected about pupils will be kept for 6 years, unless there are additional legal circumstances to be kept longer.

Rights of access to information

There are two distinct rights of access to information held by schools about pupils.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

These procedures relate to subject access requests made under the Data Protection Act 1998.

Subject Consent

In many cases, the school can only process personal data with the consent of the individual. In some cases, if the data is sensitive, as defined in the GDPR Act, express consent must be obtained.

Agreement to the school processing some specified classes of personal data is a condition of acceptance of employment for staff. This includes information about previous criminal convictions. Working within a school will bring the applicants into contact with children. The school has a duty under the Children Act 1989 and other enactments to ensure that staff are suitable for the job. The school has a duty of care to all staff and students and must therefore make sure that employees and those who use school facilities do not pose a threat or danger to other users.

The school may also ask for information about particular health needs, such as allergies to particular forms of medication, or any medical condition such as asthma or diabetes. The school will only use this information in the protection of the health and safety of the individual, but will need consent to process this data in the event of a medical emergency, for example.

Processing Sensitive Information

Sometimes it is necessary to process information about a person's health, criminal convictions, or race. This is known as personal data and data concerning health. This may be to ensure that the school is a safe place for everyone, or to operate other school policies, such as the Sick Pay Policy or the Equal Opportunities Policy. An offer of employment may be withdrawn if an individual refuses to consent to this without good reason.

Retention of Data

The school has a duty to retain some staff and student personal data for a period of time following their departure from the school, mainly for legal reasons, but also for other purposes such as being able to provide references or academic transcripts. Different categories of data will be retained for different periods of time. Data held about individuals will not be kept for longer than necessary for the purposes required.

Conclusion

Compliance with the GDPR Act is the responsibility of all members of the School. Any deliberate breach of the Data Protection Policy may lead to disciplinary action being taken, or even to a criminal prosecution.

Ref: "*The Data Protection Act 1998*"