Data Protection Policy: De La Salle College

1. Introduction and Purpose

De La Salle College is steadfast in its commitment to the fair, safe, and lawful collection, storage, and use of personal data. This policy serves as the formal framework for ensuring that the College and its entire staff body adhere to UK data protection legislation, thereby safeguarding the fundamental rights of individuals and maintaining the integrity of the institution's data processing activities.

2. Legislation and Framework

This policy is governed by the following statutory requirements and frameworks:

- The **UK General Data Protection Regulation (UK GDPR)**.
- The **Data Protection Act 2018 (DPA)**.
- The **Data Use and Access Act 2025**, representing the evolving landscape of UK data legislation.

The College further ensures that all procedures align with the Department for Education (DfE) guidance for maintained schools and academies to uphold the highest standards of educational compliance.

3. The 7 Key Data Protection Principles

De La Salle College mandates strict adherence to the seven core principles established by the UK GDPR:

1. **Lawfulness, fairness and transparency:** The College processes personal data lawfully and fairly, providing clear and accessible information to individuals regarding the use of their data.
2. **Purpose limitation:** Personal data is collected only for specified, explicit, and legitimate purposes and is never processed in a manner incompatible with those intentions.
3. **Data minimisation:** Staff must ensure that the personal data held is adequate, relevant, and strictly limited to what is necessary for the stated purpose.
4. **Accuracy:** The College maintains rigorous standards to ensure personal data is accurate and, where necessary, kept updated or corrected without delay.
5. **Storage limitation:** Information is retained in an identifiable form only for as long as is necessary to fulfil the purposes for which it was originally collected.
6. **Integrity and confidentiality (security):** The College utilizes appropriate technical and organizational measures to ensure data is protected against unauthorized access, accidental loss, or destruction.
7. **Accountability:** The College maintains comprehensive documentation and robust internal controls to demonstrate proactive compliance with all data protection principles.

4. Definition of Data Categories in a School Context

The College classifies personal information into three distinct categories to ensure appropriate levels of protection:

Personal Data

Personal data is any information relating to an identified or identifiable living individual. Within the College context, this includes identity details (names, roles), contact information, pupil behaviour and attendance records, assessment and exam results, staff recruitment information, staff contracts, **staff development reviews**, and both **staff and pupil references**.

Special Category Data

As this data is particularly sensitive, it requires heightened protection. This includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic and biometric information (such as fingerprints), health matters, and sexual orientation. In line with best practice, the College also treats information regarding safeguarding, special educational needs and disability (SEND), Pupil Premium status, Children in Need (CIN), and Children Looked After (CLA) as special category data.

Criminal Offence Data

This category covers records of criminal convictions and offences or related security measures. The College processes this data when storing the outcomes of Disclosure and Barring Service (DBS) checks for employees, non-employed staff, and volunteers. Explicitly, the storage of a DBS outcome—even if the check is clear and reveals no convictions—constitutes the processing of criminal offence data.

5. Data Subjects

The College processes personal data relating to several groups of individuals, including:

- Pupils and former pupils.
- Parents and carers.
- Employees, non-employed staff, and **applicants (for both staff and pupil roles)**.
- Governors, trustees, and volunteers.
- Local authority personnel and visitors.

6. Subject Access Requests (SARs) and Information Rights

A Subject Access Request (SAR) is a formal information rights request that allows individuals to obtain a copy of the personal data the College holds about them. This

right extends to parents or guardians requesting data held about individuals for whom they have parental responsibility.

The College is legally obligated to respond to these requests within statutory timeframes. Beyond SARs, individuals possess the right to request the rectification, erasure, or restriction of their personal information.

7. Handling Personal Data Breaches

A personal data breach is a security incident resulting in data being lost, stolen, destroyed, altered, or accessed without authorization. In the event of a suspected breach, staff must act with extreme urgency to meet the statutory **72-hour** notification window:

1. **Recognise the incident:** Identify potential compromises, such as a lost mobile device, an incorrectly addressed email containing sensitive data, or unauthorized system access.
2. **Report the incident:** Immediately notify the Data Protection Officer (DPO) or the designated internal authority to initiate the formal response protocol.
3. **Follow good practice procedures:** Cooperate fully with the DPO to mitigate the impact of the breach, notify affected individuals where necessary, and document the recovery steps.

8. Record Keeping and Management

The College conducts regular audits to monitor the personal data it processes. To uphold the "storage limitation" principle, the College adheres to a formal **data retention schedule**. This schedule documents the mandatory lifespan of various data assets before they are securely destroyed. Staff can access the full retention schedule via the **Staff Portal**.

9. Security and Data Assets

Personal data is held within "data assets," which the College categorizes as:

- **Data items:** Single pieces of information.
- **Data item groups:** Data items related to the same process.
- **Data sets:** Related data collections manipulated as a unit.
- **Systems:** Specific administrative software.
- **System groups:** The larger platforms housing administrative software.

In accordance with the principle of "Integrity and Confidentiality," all data assets must be processed using secure systems and protocols to prevent unauthorized access and ensure the privacy of all data subjects.