DATA PROTECTION

Policy applies from EYFS to Sixth Form and to all Staff and parents	
Date policy reviewed:	21.01.2025
Date of next review:	15.01.2026
Version:	01.25 v1
Author:	Mr Michael Stewart

Version	Date	Paragraph	Material change	Approval
12.22 v1	02.12.2022	7 9 11	Additional detail re. lawful processing added. Additional detail re rights of an individual added. Section updated re. requirements for staff who process credit card data.	Mr Michael Stewart
01.24 v1	15.01.2024	9 and 10	New section inserted re. third parties and section re. rights of an individual updated.	Mr Michael Stewart
01.25 v1	21.01.2025	N/a	No material amendments.	Mr Michael Stewart

Clifton High School is committed to child protection and safeguarding children and young people and expects all staff, visitors and volunteers to share this commitment.

Related Policies
Child Protection and Safeguarding
Complaints
Data Breach
Data Protection Impact Assessment
Data Retention and Disposal
Online Safety
Privacy Notices
Staff Acceptable Use of Information Communication Technology Agreement
Taking, Storing and Using Images of Children – Parents and Staff

1. Introduction

Clifton High School holds a large amount of personal and sensitive data. Every care must be taken by staff to protect all personal and sensitive data held by the School. This policy sets out the School's expectations and procedures with respect to processing any personal data we collect from data subjects (including parents, pupils, employees, contractors and third parties).

2. Legal Context

Data protection is an important legal compliance issue for Clifton High School. During the course of the School's activities it collects, stores and processes personal data (sometimes sensitive in nature) about staff, pupils, parents, alumni, contractors and other third parties who come into contact with the School, in a manner more fully detailed in the School's Privacy Notices. The School, as 'data controller' (as defined in section 3 below) is liable for the actions of its staff in how data is handled. All staff have a part to plan in ensuring the School complies with, and is mindful of, the legal obligations, whether that personal data handling is routine or sensitive.

UK data protection law consists primarily of the UK General Data Protection Regulation (**UK GDPR**) and the Data Protection Act 2018 (**DPA 2018**) (together **data protection law**). The DPA 2018 includes specific provisions of relevance to independent schools, in particular in relation to safeguarding obligations and the right of access to personal data.

Data protection law has strengthened the rights of individuals and placed tougher compliance obligations on organisations that handle personal data, including schools. The Information Commissioner's Office (**ICO**) is responsible for enforcing data protection law, and will typically look into individuals' complaints routinely and without cost, and has various powers to act for breaches of the law.

3. Definitions

Data controller – a person or body that determines the purpose and means of the processing of personal data, and who is legally responsible for how it is used. The School is a data controller. An independent contractor who makes their own such decisions is also, separately, likely to be a data controller.

Data processor – an organisation that processes personal data on behalf of a data controller, for example a payroll or IT provider or other supplier of services with whom personal data may be shared but who is not authorised to make any decisions about how it is used.

Data subject: the identified or identifiable living individual to whom personal data relates.

Personal data breach – a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Personal information (or '**personal data**') – any information relating to a data subject by which that individual may be identified by the data controller. That is not simply a name but any form of identifier, digital or contextual, including unique ID numbers, initials, job titles or nicknames. Note that personal information will be created almost constantly in the ordinary course of work duties (such as in emails, notes of calls, and minutes of meetings). The definition includes expressions of opinion about the individual or any indication of the School's, or any person's, intentions towards that individual.

Processing – virtually anything done with personal information, including obtaining or collecting it, structuring it, analysing it, storing it, sharing it internally or with third parties (including making it available to be viewed electronically or otherwise), altering it or deleting it.

Special categories of personal data – data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health and medical conditions, sex life or sexual orientation, genetic or biometric data used to identify an individual. There are also separate rules for the processing of personal data relating to criminal convictions and offences.

Staff – for the purpose of this policy, 'staff' is applied widely and refers to all current Governors, employees, workers, volunteers, and contractors, who may be employed or engaged by the School to work for it in any capacity. This policy is not intended to confer worker or employee status but represents a set of standards and safeguards for data protection that all staff (including volunteers and contractors) are expected to meet.

4. Who does this policy apply to?

All members of staff are required to comply with this policy when they handle personal data. Breaches of this policy may result in disciplinary action. Accidental breaches in handling personal data, for example by human error, will not always be treated as a disciplinary issue. However, failure to report breaches that pose significant risks to the School or individuals will be considered a serious matter.

In addition, this policy represents the standard of compliance expected of those who handle the School's personal data as contractors, whether they are acting as "data processors" on the School's behalf (in which case they will be subject to binding contractual terms relating to data protection) or as data controllers responsible for handling such personal data in their own right.

Where the School shares personal data with third party data controllers (which may include other schools, parents, appropriate authorities) each party will need a lawful basis to process

that personal data and will be expected to do so lawfully and with due regard to security and confidentiality, as set out in this policy.

Volunteers and contractors are data controllers in their own right, and the same legal regime and best practice standards set out in this policy apply to them.

5. Person responsible for Data Protection at the School

Clifton High School is registered as a data controller with the ICO. The School's ICO number is Z7520007.

The School has appointed the Finance Director as the Data Protection Lead, whose role it is to monitor that all personal data is processed in compliance with this policy and data protection law. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Lead.

6. The Principles

UK GDPR sets out six principles relating to the processing of personal data which must be adhered to by data controllers (and data processors). These require that personal data must be:

- processed **lawfully**, **fairly** and in a **transparent** manner;
- collected for **specific and explicit purposes** and only for the purposes it was collected for;
- **relevant** and **limited** to what is necessary for the purposes it is processed;
  accurate and kept **up to date;**
- **kept for no longer than is necessary** for the purposes for which it is processed; and
- processed in a manner that ensures **appropriate security** of the personal data.

UK GDPR's broader 'accountability' principle also requires that the School not only processes personal data in a fair and legal manner but can demonstrate that the processing is lawful. This involves, among other things:

- keeping records of data processing activities, including by way of logs and policies;
- documenting significant decisions and assessments about how personal data is used (including via formal risk assessment documents called Data Protection Impact Assessments); and
- having an 'audit trail' vis-à-vis data protection and privacy matters, including for example when and how our Privacy Notices were updated; when staff training was undertaken; how and when any data protection consents were collected from individuals; how personal data breaches were dealt with, whether or not reported (and to whom), etc.

7. Lawful grounds for data processing

Under the UK GDPR there are several different lawful grounds for processing personal data. These include:

- **Consent**. The individual has given clear consent for the School to process their personal data for a specific purpose. The bar for what constitutes consent under UK GDPR is relatively high and can be withdrawn by the data subject. For those reasons, it is considered preferable for the School to rely on another lawful ground where possible.
- **'Legitimate interests.** ' The processing is necessary for the School's legitimate interests or the legitimate interests of a third party. This is the most flexible basis for processing. However, it requires transparency and a balancing assessment to be made between the rights of the individual and the interests of the School. It can be challenged by data subjects and also means the School is taking on extra responsibility for considering and protecting people's rights and interests. The School's legitimate interests are set out in its Privacy Notices, as required by data protection law.
- **Compliance with a legal obligation** . The processing is necessary for the School to comply with the law. This includes in connection with employment, engagement of services and diversity.
- **Contractual necessity.** The processing is necessary for the School to comply with the terms of a contract which it has with the individual e.g. to perform a contract with staff or parents, or the engagement of contractors.

There is also a narrower set of grounds for processing special categories of personal data (such as health information), which includes explicit consent, emergencies, and specific public interest grounds.

8. Responsibilities of Staff

8.1 Record-keeping

It is important that personal data held by the School is accurate, fair and adequate. Staff are required to speak to an appropriate member of staff if they believe that any personal data is inaccurate or untrue or they are dissatisfied with how it is recorded. This applies to how staff record their own data, and the personal data of others – in particular colleagues, pupils and their parents – in a way that is professional and appropriate.

Staff should be aware of the rights set out in section 10 (Rights of Individuals), whereby any individual about whom a member of staff records information on School business (notably in emails and notes) digitally or in hard copy files, may have the right to see that information. This must not discourage staff from recording necessary and sometimes difficult records of incidents or conversations involving colleagues, pupils or parents, in accordance with the School's other policies, and grounds may sometimes exist to withhold this data from such

requests. However, the starting position for staff is to record every document or email in a form they would be prepared to stand by should the person about whom it was recorded ask to see it.

8.2 Data handling – responsible processing

All staff have a responsibility to handle the personal data which they encounter fairly, lawfully, responsibly and securely and in accordance with all relevant School policies and procedures (to the extent applicable to them). In particular, there are data protection implications across a number of areas of the School's wider responsibilities, such as safeguarding and IT security, so all staff should read and comply with all the Related Policies listed at the start of this policy.

Responsible processing also extends to the creation and generation of new personal data/records, which should always be done fairly, lawfully, responsibly and securely.

8.3 Avoiding, mitigating and reporting data breaches

One of the key obligations contained in data protection law is on reporting personal data breaches.

Data controllers must report personal data breaches to the ICO within 72 hours if the breach is likely to result in a risk to the rights and freedoms of the individual. The School must keep a record of all personal data breaches, regardless of whether ICO is notified to ensure that it can justify its decision not to report the breach. In addition, controllers must notify individuals affected if the breach is likely to result in a "high risk" to their rights and freedoms.

If staff become aware of a personal data breach, they must notify the Data Protection Lead or, in their absence, a member of Senior Leadership. If staff are in any doubt as to whether to report something internally, it is always best to do so. A personal data breach may be serious, or it may be minor; and it may involve fault or not; but the School always needs to know about them to make a decision. The School may not need to treat the data protection breach itself as a disciplinary matter, but a failure to report a breach could result in significant exposure for the School and for those affected, and as such it could be treated as a serious disciplinary matter.

The steps to be taken by the School should staff report a breach are set out in the Data Breach Policy.

8.4 Care and data security

All staff are required to remain mindful of the data protection principles outlined in section 6 above and to use their best efforts to comply with those principles whenever they process personal information. Data security is not simply an online or digital issue but one that affects daily processes, including filing and sending correspondence (notably hard copy documents).

Data processors should always consider what the most assured and secure means of delivery is, and what the consequences would be of loss or unauthorised access.

Staff with management/leadership responsibilities must be particular champions of the data protection principles and oversee the swift reporting of any concerns about how personal information is used by the School to the Data Protection Lead or a member of the Senior Leadership Team, and to identity the need for (and implement) regular staff training. Staff must attend any training when required.

9. Use of third-party platforms/suppliers

Where a third party is processing personal data on the School's behalf it is likely to be a data 'processor', and this engagement must be subject to appropriate due diligence and contractual arrangements as required by the UK GDPR. It may also be necessary to complete a DPIA before proceeding, particularly if the platform or software involves any sort of novel or high-risk form of processing (including any use of artificial intelligence ("AI") technology). Staff should refer to and follow the Data Protection Impact Assessment Policy.

10. Rights of Individuals

In addition to the School's responsibilities when processing personal data, individuals have certain specific rights, perhaps most significantly that of access to their personal data held by a controller (i.e. the School). This is known as the 'subject access right' (or the right to make 'subject access requests'). Such a request must be dealt with promptly and does not need any formality, nor does it need to refer to the correct legislation.

The School will respond to Subject Access Requests (**SARs**) in accordance with data protection law and its own internal procedures for dealing with such requests. To avoid personal data about one individual being sent to someone who is not entitled to it, the School will verify the identity of the applicant. The School does not charge for processing a SAR. The statutory response time is one month. The School shall keep a log of all SARS received.
Individuals also have legal rights under the DPA 2018 to:

- Be informed about how data is being used.
- Correct the personal data held about them if it is inaccurate or incomplete.
- Have their personal data erased (in certain circumstances).
- Stop or restrict processing of their personal data (in certain circumstances).
- Obtain and reuse their personal data for their own purposes.
- Object to a particular way the School processes their data where the individual feels this has a disproportionate impact on them.

None of the above rights for individuals are unqualified and exceptions may well apply. However, certain other rights of an individual are absolute under the UK GDPR and must be respected, specifically the right to:

- Object to automated individual decision-making and profiling (i.e. where a significant decision is made about the individual without human intervention).
- Object to direct marketing.
- Withdraw consent where it is relied on for processing personal data (without affecting the lawfulness of processing carried out prior to that point in reliance on consent, or of any processing carried out on some other legal basis other than consent).

If you receive a request from an individual who is purporting to exercise one or more of their data protection rights, you must tell the Data Protection Lead or a member of Senior Leadership as soon as possible.

11. Data security: online and digital

The School shall ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

Details of the particular security measures staff should adhere to in respect of the use of ICT are set out in the Staff Acceptable Use of Information Communication Technology Agreement. Staff should not provide personal data to third parties, including a volunteer or contractor, unless there is a lawful reason to do so. The use of personal email accounts by staff for School business is not permitted other than with permission of the Data Protection Lead.

If staff are in any doubt as to the application of these requirements, they should contact the Data Protection Lead for further advice before proceeding.

12. Processing of financial/credit card data

The School complies with the requirements of the PCI Data Security Standard (PCI DSS). Staff who are required to process credit card data must ensure that they are aware of and comply with the most up to date PCI DSS requirements. If further guidance is required, please refer to the Finance Director.

Other categories of financial information, including bank details and salary, or information commonly used in identity theft (such as national insurance numbers or passport details) may not be treated as legally sensitive but can have material impact on individuals and should be handled accordingly.

13. Complaints

If an individual believes the School has not complied with this policy or acted otherwise than in accordance with data protection law, then the complaint will be dealt with in accordance with the School's Complaints Policy, or in accordance with the provisions of the contractual terms governing data processing.

Further advice and information are available from the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. www.ico.gov.uk or telephone 01625 5457453.