Colyton Grammar School
DATA PROTECTION POLICY

1. Introduction

Colyton Grammar School has to collect and use information about the people with whom we work in order to operate effectively and efficiently. This may include students and their families, members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition the School may be required by law to collect and use information in order to comply with the requirements of central government.

The School is firmly committed to handling and dealing with all personal information properly, no matter how it is collected, recorded and used, and whether it is on paper, in computer records or recorded by any other means.

The School regards the lawful and correct treatment of personal information as critical to its successful operations, maintaining confidence between the School and those with whom it carries out business. The School will ensure that it treats personal information correctly in accordance with the law.

The School fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 1998 (DPA).

This policy sets out the principles of data protection, the School's responsibilities, the access rights of individuals and issues relating information sharing and complaints.

2. Scope

This policy applies to all employees, governors, contractors, agents and representatives and temporary staff, working for or on behalf of the School.

This policy applies to all personal information created or held by the School, in whatever format (e.g. paper, electronic, email, film) and however it is stored (e.g. ICT systems, databases, email, filing cabinet, shelving and personal filing drawers)

The DPA does not apply to requests for information about a person if they are deceased. These requests should be processed in accordance with the Freedom of Information Act (FoIA) 2000, but should also be considered fairly and lawfully.

3. The principles of data protection

The DPA stipulates that anyone processing personal data must comply with **eight principles** of good practice. These principles are legally enforceable.

The principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes;
3. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. 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.

The DPA provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **"sensitive" personal data** (see glossary for definitions). Sensitive personal data requires stricter conditions of processing.

4. Responsibilities
Colyton Grammar School is a **data controller** under the Data Protection Act 1998.

The Governors' Chairs' Committee is responsible for ensuring compliance with this policy and has delegated the responsibility for managing Data Protection to the nominated Data Protection Officer.

The Data Protection Officer is responsible for ensuring that the appropriate processes and procedures are in place to comply with the DPA and this policy. He/she is responsible for ensuring that data is appropriately protected or that controls are in place to prevent access by unauthorised personnel, and that data cannot be tampered with, lost or damaged. The Data Protection Officer is also responsible for providing day to day advice and guidance to support the School in complying with the DPA and this policy.

All members of staff, contractors and governors who hold or collect personal data are responsible for their own compliance with the DPA and must ensure that personal and/or sensitive information is kept and processed in accordance with the DPA and this policy. In particular, staff must not attempt to access personal data that they are not authorised to view. Failure to comply with the DPA may result in disciplinary action which could further lead to dismissal and, in some cases, criminal proceedings/prosecution.

5. Related policies
This policy should be read in conjunction with

- The Subject Access Policy
- The Freedom of Information Act Policy and Publication Scheme

6. Agents, partner organisations and contractors
If a contractor, partner organisation or agent of the School is appointed or engaged to collect, hold, process or deal with personal data on behalf of the School, or if they will do so as part of the services they provide to the School, the Data Protection Officer must ensure that personal data is kept in accordance with the principles of the DPA and this policy.

Security and Data Protection requirements must be included in any contract that the agent, contractor or partner organisation enters into with the School.

A data confidentiality agreement must be in place prior to any work commencing.

The School promotes information sharing where it is in the best interests of the data subject. Where information sharing protocols are in place, the School will comply with the standards established in those protocols.

7. Access rights by individuals - subject access requests (SARs)
An individual may request a copy of any data held about them, or information about the reasons for which it is kept and processed. This is called a Subject Access Request under the DPA.

The School has a Subject Access Policy and supporting procedures that comply with the principles of the DPA. These can be found on the website at Data Protection Act

8. Disclosure of personal information about third parties
Personal data must not be disclosed about a third party, except in accordance with the DPA.

9. Information sharing
The School may share information when it is in the best interests of the data subject and when failure to

share data may carry risks to vulnerable groups and individuals. This must be done in a secure and appropriate manner. The School will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards.

10. Data quality, integrity and retention
If an individual requests that personal data held about them be updated because it is wrong, incomplete or inaccurate, the position should be investigated thoroughly, with reference to the source of information. A caution should be marked on the person's file to indicate uncertainty regarding accuracy until the investigation is complete. The School will work with the person to either correct the data and/or allay their concerns. An individual is entitled to apply to the court for a correcting order which would authorise the School to rectify, block, erase or destroy the inaccurate information as appropriate.

Individuals can request the School to stop processing data. If data is properly held for marketing purposes for example, an individual is entitled to require that this is discontinued as soon as possible. Requests must be made in writing, but generally all written or oral requests should be heeded as soon as they are made. The individual must be informed in writing that the processing has been discontinued.

If data is held for any other purposes, an individual may request that processing ceases if it is causing them unwarranted harm or distress. This does not apply if they have given their consent, if the data is held in connection with a contract with the person, if the School is fulfilling a legal requirement, or, if the person's vital interests are being protected. Valid written requests must be responded to in writing within 21 calendar days upon receipt.

11. Complaints
Complaints about how the School processes data under the DPA and responses to subject access requests are dealt with using the School's Complaints Procedure. This can be found in the School Policies section of the school website.

12. Notification
The DPA requires every data controller processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence. The Information Commissioner maintains a public register of data controllers, in which Colyton Grammar School is registered.
The Data Protection Officer will review and update the Data Protection Register annually prior to notification to the Information Commissioner. Staff and governors should notify the Data Protection Officer of any change to the processing of personal data between annual reviews.

13. Breach of policy
The School will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated and judged on its individual circumstances, addressed accordingly and carried out in line with the employee code of conduct, or with School policies and procedures as appropriate.

14. Equality Impact Assessment
No issues relating to protected characteristics under equality legislation have been identified in this policy.

15. Consultation
The following have been consulted in the preparation and review of this policy:

- Senior Leadership Team
- Network Manager
- Data Protection Officer

16. Review of policy
This policy will be reviewed on at least a three yearly basis.