Policy Statements and Procedures

DATA PROTECTION POLICY

1. INTRODUCTION

This policy applies to all personal data held by Hewens College. It encompasses paper records; data held on computer and associated equipment, including CCTV, of whatever type and at whatever location, used by or on behalf of Hewens College.

The obligations outlined in this policy apply to all those who have access to personal data, whether they are employees, governors, employees of associated organisations or temporary staff. It includes those who work at home or from home, who must follow the same procedures as they would in an office environment.

Any individual who knowingly or recklessly processes data for purposes other than those for which it is intended or makes an unauthorised disclosure is liable to prosecution. All individuals permitted to access personal data must agree to comply with this policy.

The guidance displayed on the Information Commissioner's website (www.dataprotection.gov.uk) and published in "the Guide to Data Protection" published by the Information Commissioner's office is available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

2. POLICY OBJECTIVES

Hewens College will comply with the terms of the Data Protection Act 1998 and any subsequent relevant legislation, to ensure personal data is treated in a manner that is fair and lawful.

3. PRINCIPLES

The eight enforceable principles of good practice contained in the Data Protection Act 1998. These state that personal data must be:

- Fairly and lawfully processed;
- Obtained only for one or more specified and lawful purposes;
- Adequate, relevant and not excessive in relation to the purpose for which it is processed;
- Accurate and kept up to date;
- Not kept for longer than is necessary;
- Processed in accordance with the data subject's rights;

- Secure;
- Not transferred to a country outside the EEC unless that country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Confidentiality and Security:

Personal data is confidential and confidentiality must be preserved in compliance with the Data protection Principles as defined in the Data Protection Act 1998.

Paper records will be managed so that access is restricted to those who need to use the information and stored in secure locations to prevent unauthorised access.

Computer systems will be designed and computer files created with adequate security levels to preserve confidentiality. Those who use the College's computer equipment will have access only to the data that is both necessary for the work they are doing and held for carrying out that work.

Training:

All members of staff who work with personal data, and their line managers, will receive appropriate training in the area of Data Protection.

4. PROCEDURE

Data Gathering:

Only relevant personal data may be collected and the person from whom it is collected will be informed why the data is being collected, of the data's intended use and any possible disclosures of the information that may be made.

Privacy notices will be issued to all persons from whom personal data is collected. Two versions will be used; one in respect of students' personal data and the other in respect of all other persons' personal data.

Processing:

All processing of personal data in each college within the Trust will comply with the Data Protection Principles as defined in the Data Protection Act 1998.

In the situation where data is processed by a third party, the third party will be required to act in a manner that ensures compliance with the Data Protection Act 1998.

Data will only be processed for the purpose for which it was collected and will not be used for incompatible purposes without the consent of the data subject.

Data Storage:

Each College within the Trust will hold the minimum amount of personal data necessary to enable it to perform its functions. The data will be erased once the need to hold it has passed.
Each College within the Trust will store personal data in a secure and safe manner.

Electronic data will be protected by standard password and firewall systems operated by the approved supplier of IT services for all colleges within the Trust.

Personal data, the loss of which could cause damage or distress to individuals, which is used or stored on portable or mobile devices will be encrypted using encryption software which meets the current standard or equivalent. This applies to all laptop computers and portable memory devices (including memory sticks etc.)

Computer workstations in administrative areas will be positioned so that they are not visible to casual observers.

Manual data will be stored where it is not accessible to anyone who does not have a legitimate reason to view or process that data.

Particular attention will be paid to the need for security of sensitive personal data.

Data Checking:

Each college within the Trust will issue regular reminders to staff and parents, guardians and carers to ensure that personal data held is up-to-date and accurate.

Any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

Data Disclosures:

Personal data will only be disclosed to organisations or individuals for whom consent has been given to receive the data, or organisations that have a legal right to receive the data without consent being given.

When requests to disclose personal data are received by telephone it is the responsibility of the member of staff taking the call to ensure the caller is entitled to receive the data and that they are who they say they are. This should be done by calling them back, preferably via a switchboard, to ensure the possibility of fraud is minimised.

If a personal request is made for personal data to be disclosed it is again the responsibility of the member of staff to ensure the caller is entitled to receive the data and that they are who they say they are. If the person is not known personally, proof of identity should be requested.

Requests from parents, guardians, carers or students for printed lists of the names of students in particular groups, which are frequently sought at special times of the year such as Christmas, should be politely refused as permission would be needed from all the data subjects contained in the list.

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

Routine consent issues will be incorporated into colleges' student data gathering sheets, to avoid the need for frequent, similar requests for consent being made by the college or the Trust.

Personal data will only be disclosed to Police Officers if they are able to supply a relevant document which notifies of a specific, legitimate need to have access to specific personal data.

A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Subject Access Requests:

If a college within the Trust receives a written request from a data subject to see any or all personal data that the College and/or Trust holds about them this will be treated as a legitimate Subject Access
Request and the College or Trust will respond within the recommended 40 day deadline.

Informal requests to view or have copies of personal data will be dealt with wherever possible at a mutually convenient time but, in the event of any disagreement over this, the person requesting the data will be instructed to make their application in writing and the College/Trust will comply with its duty to respond within the 40 day time limit.

Data Protection statements will be included in the prospectus of all colleges across the Trust and on all forms that are used to collect personal data.

5. MONITORING AND REVIEW

This policy will be kept under review in order to keep it in line with relevant legislation.

6. ROLES AND RESPONSIBILITIES

Ownership of Data:

Each college Alliance or department within the Trust is responsible for the personal data that it holds.
This responsibility extends to any data that is processed by a third party. The Alliance or department will hold a record of all data files that it owns containing personal data, whether on paper or electronic media. Where required, the Alliance or department will provide the necessary information to the Executive Principal to facilitate the notification of the data to the Information Commissioner.

The governors of the Academy Board have delegated the Principal as the person who has overall responsibility for compliance with the Data Protection Act within their setting.

7. LINKS TO OTHER POLICIES AND DOCUMENTS

This policy links with:

- ICT Policy
- Cyber Security Policy
- Policies included in the Examinations Folder
- Complaints Policy

Updated	October 2025
Next Review Date	September 2026