Policy name:	Data Protection Policy
Author(s) :	Anna Holt/Andy Moss
Owner :	Anna Holt/Andy Moss
Date written:	May 2022
Status:	
Date approved:	June 20
Current version review date:	June 22

Version	Date	Control reason

Linked to other policies	Owner
Freedom of Information	AHO
Staff and Student Privacy Notices	AHO/AMO
Staff Code of Conduct	LBA
CCTV policy	CGR

Aquinas College, through its policies and day to day work is committed to promoting equality and fairness. This applies to everyone, regardless of gender, racial or ethnic background, disability, religion, sexual orientation or age and embraces the College's legal responsibility.
The persons/group responsible for this document reserve the right to amend this document at any time should the need arise. All appropriate staff will be informed should this occur.

Data Protection Policy

1. Data protection policy statement

1.1 Aquinas College (the College) takes its responsibilities with regard to the requirements of Data Protection seriously and responsibly. On 25th May 2018 the Data Protection Act 1998 was superseded in the UK by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA), which provides individuals with enhanced rights, and imposes increased responsibilities on organisations processing personal data. This statement applies under both the DPA and GDPR.

2. Purpose and scope of the policy

2.1 To provide a Data Protection Policy for Aquinas College which complies with the requirements of the Data Protection Act 2018.

2.2 The College is the data controller for all personal data that it holds and processes, except where it is done in the capacity of a data processor on behalf of another data controller. This statement establishes the College's procedures governing the collection and release of student data and is provided to students at the application and enrolment stages. It includes information about how student data is used, and where it is supplied by the College to the Educations and Skills Funding Agency (ESFA) and other external parties.

This statement also establishes the procedures governing the collection and use of staff data and is made available to new staff on induction.In addition it:

(a) Covers the processing of all personal information of students and staff whose use is controlled by the College.

(b) Covers all personal information of students and staff that is handled, stored, processed or shared by the College, whether organised and stored in physical or IT based record systems. As such, the Act covers all personal data that is held electronically, including databases and email as well as paper records.

(c) Applies to all staff, students, contractors, partnership organisations and partner staff of Aquinas College.

2.3 Aquinas College adheres to the principles of data protection stated in the Data Protection Act 2018. In accordance with these principles the College assures that personal data shall be:

- Processed fairly and lawfully
- Processed for specific purposes only
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than necessary
- Processed in accordance with the data subjects' rights
- Processed and held securely

2.4 Aquinas College and its staff, students, contractors, partner organisations and partner staff that process or use personal data on behalf of the College must comply with these principles and ensure that they are followed at all times.

2.5 Information Commissioner's Office; The details of the College's registration are as follows:

Registration Number: Z606811X

Registration Expires: 30 January 2023

Data Controller: Aquinas Sixth Form College

Address: Nangreave Road Stockport SK2 6TH

3. Responsibilities

3.1 Aquinas College complies with the regulations of the Data Protection Act (2018), and as such is registered (as a data controller who is processing information) with the Information Commissioners Office (ICO).

3.2 Staff of the College who process personal data concerning students, staff, applicants, alumni or any other individual must comply with the requirements of this policy. All members of staff must ensure that:

- All personal data is kept securely
- No personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party
- Any queries regarding data protection, including subject access requests and complaints, are promptly directed to the College's Data Protection Officer
- Any data protection breaches are swiftly brought to the attention of the Data Protection Officer and that support is given in resolving breaches
- Where there is uncertainty around a data protection matter advice is sought from the Data Protection Officer

3.3 Where members of staff are responsible for supervising students' work which involves the processing of personal information, they must ensure that students are made aware of the requirements of the Data Protection Act 2018. The particular requirement to obtain consent from a third party, where appropriate, must be adhered to.

3.3 Students are required to ensure that where they provide their own personal data to the College, that it is accurate and up to date.

3.4 Where external companies are used to process personal data on behalf of Aquinas College, responsibility for security and appropriate use of the data remains with the College.

3.5 Aquinas College is responsible for the use made of personal data by anyone working on its behalf including contractors, short-term and voluntary staff. Where the College employs short term contractors, short term staff and voluntary staff it must ensure that they appropriately screened and approved for the data they will be using and processing.

4. Data security

4.1 All staff, contractors, partner organisations and partner staff must ensure that any personal information which they hold is kept securely and that they take appropriate precautions by seeking to ensure the following:

- Documents containing personal information are kept in a lockable cabinet or room
- Data held electronically on computer is password protected
- Data kept on discs or data storage devices are stored securely and are encrypted
- Individual passwords are kept confidential and not disclosed to others
- Computers are not left unattended where data is visible on the screen to other people
- Paper based records are never left where unauthorised personnel can read or gain access to them

4.2 When manual records are no longer required they should be shredded or confidentially bagged and disposed of securely.

5. CCTV

5.1 We use CCTV in various locations around the College site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

5.2 We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

6. Photographs and videos

6.1 As part of the College activities, we may take photographs and record images of individuals within the College.

6.2 We will obtain written consent from students for photographs and videos to be taken of them for communication, educational, marketing and promotional materials.

6.3 Uses may include:

- Within the College on notice boards and College magazines, brochures, newsletters, etc.
- Outside the College for marketing purposes, on the College website or social media pages.

6.4 Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further

7. Rights of individuals

7.1 The Data Protection Act provides the individual whose personal data and sensitive personal data/special category data is held by the College, with the following rights:

a. The right to request access to their personal data held by the College (subject access request).

b. The right to have inaccurate or incomplete personal data rectified.

c. The right to erasure of personal data – this will only apply where there is no legitimate reason for the College to continue to process the personal data.

d. The right to restrict the processing of personal data – individuals have the right to block the processing of their personal data by the College in specific situations.

e. The right to data portability – students have the right to request provision of some elements of their information (for example academic progress details) in digital form in order to provide it to other organisations.

f. The right to object – students can object to the processing of their personal data by the College in certain circumstances, including the sending and receiving of direct marketing material.

g. The right to object to automated decision making and profiling – individuals have the right to object to decisions taken by automatic means without human intervention in some circumstances.

7.2 All requests to exercise any of these rights should be made to the College's Data Protection Officer.

7.3 Where the processing of personal data or sensitive personal data/special category data is based on the non-contractual consent of the student, they have the right to withdraw their consent at any time by contacting the department or service who obtained that consent or the College's Data Protection Officer.

8. Subject access requests

8.1 Subject access requests must be submitted in writing, either by letter or email to the Data Protection Officer. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested

8.2 If staff receive a subject access request they must immediately forward it to the Data Protection Officer.

8.3 When responding to subject access requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge in most cases May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary.

8.4 If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee that takes into account administrative costs.

9. Retention and disposal of data

9.1 Aquinas College is not permitted to keep personal information of either students or staff for longer than is required for its purpose. However, some data will be kept longer or in perpetuity to comply with statutory or funding body requirements.

9.2 A basic academic record for individual students will be kept permanently by the College, with more detailed records kept for defined retention periods. Details of the retention of student records are shown in the Privacy Notice made available to students on application, and enrolment.

9.3 Basic staff records are kept in perpetuity to enable provision of references on request. Detailed staff records, including medical or disciplinary information, will kept for the financial year of departure from College employment plus six years.

9.4 Personal and confidential information will be disposed of by means that protect the rights of those individuals. This will be achieved by shredding, disposal of confidential waste or secure electronic deletion, as appropriate.

10. Data protection breaches

10.1 Where a data protection breach occurs, or is suspected to have occurred, the Data Protection Officer should be notified as soon as possible. The Data Protection Officer will work with appropriate staff in the College to:

- Minimise the damage
- Assess the extent of the damage and determine appropriate action
- Notify individuals, as appropriate
- Ascertain how the breach occurred and, if appropriate, determine how to prevent or minimise the risk of future breaches
- When appropriate, report the data breach to the ICO within 72 hours.

11. Complaints

11.1 Aquinas College is committed to being compliant with the Data Protection Act. If a student or staff member is unhappy with the College's handling of their personal data, or believes that the requirements of the DPA or GDPR may not have been fully complied with, they should contact the College's Data Protection Officer in the first instance. The College's formal complaint procedure can be invoked if appropriate, and they also have the right to submit a complaint to the Information Commissioner's Office; further details can be found at www.ico.org.uk.

12. Monitoring and Evaluation

This policy is reviewed annually to ensure it is line with any changes made to legislation. Significant changes will be taken to Governors but the normal period for Governor approval is 2/3 years?