Quarrydale Academy

Data Protection Policy

This data protection policy will be reviewed annually by the pupil and personnel committee of the governing body.

Date of last review: Spring 2018
Date of next review: Spring 2019

Policy Statement

The Academy is committed to a policy of protecting the rights and privacy of individuals (including students, staff and others) in accordance with the General Data Protection Regulation (GDPR).

The Academy needs to process certain information about staff, students and other individuals that they have dealings with for administrative purposes, e.g. to recruit and pay staff, to administer programmes of study, to record progress, to agree awards, to collect fees, and to comply with legal obligations to funding bodies and the government.

To comply with the GDPR, there must be a lawful basis for processing any individual's information, that information must be stored and processed safely and securely and it must not be disclosed to any third party without having a lawful basis to do so.

This policy applies to all staff and students of the Academy, governors and volunteers, as well as partners and companies with which the Academy undertakes it business. Any breach of the General Data Protection Regulation or the Academy's Data Protection Policy is considered to be an offence and in that event, the Academy's disciplinary procedures will apply.

As a matter of good practice, other agencies and individuals working with the Academy and who have access to personal information (i.e. External Data Processors), will be expected to have read and comply with this data protection policy and the GDPR. It is expected that members of the Academy community who deal with external agencies will take responsibility for ensuring that such agencies give written confirmation of GDPR compliance.

Background to the General Data Protection Regulation and Responsibilities

The purpose of the General Data Protection Regulation which came into force on 25 May 2018 is to protect the rights and privacy of individuals and to ensure that there is a lawful basis for processing their personal data (see article 6 and article 9 below).

The Academy, as a corporate body is the registered Data Controller with the Information Commissioner under the GDPR.

A Data Protection Officer has been appointed who is responsible for day-to-day data protection matters, for the processing of personal data with the Information Commissioner's Office, for the observation of the GDPR principles, and for developing specific guidance notes on data protection issues for members of the Academy. They will also ensure that the rights of people about whom information is held can be fully exercised under the GDPR. The Data Protection Officer is Mr Jon Smart jsmart@quarrydale.notts.sch.uk

The Academy, working with the Data Protection Officer, has identified where significant data processing takes place and where data processing mapping exercises should be carried out under this policy and to assist the Academy's compliance with the GDPR:

- Core management information
- Curriculum tools
- Payment systems
- Virtual learning environments
- Communication
- Catering
- Photographs
- ID management / biometrics
- Safeguarding
- Admissions
- Behaviour management systems
- SEND
- CPOMS (Safeguarding and Child protection software for schools)
- Governance
- Employment

The key Internal Data Processors for the various types of information being held in the list above are:

- Staff and employment Information – HR Manager
- Student assessment data – Examinations and Data Manager
- General student information and admissions – Student Services Team
- SENCO student information – SENCO(s)
- Student safeguarding information – Senior Designated Person(s)
- Student attendance information – Attendance Officer(s)
- Governance – Clerk to the Governors

- Payment systems and core management information – Business Manager
- Catering – Catering Manager
- Virtual learning environments and other ICT systems – ICT Manager
- Behaviour management systems – Deputy Headteacher, Alternative Curriculum Manager, ICT Manager, Behaviour Manager, HoY(s), all other users
- Communication – potentially all staff

The Internal Data Processors will manage and address risks to the information and will understand:

- What information is held and for what purpose
- What the lawful basis is for processing the information (see article 6 and article 9 below)
- How information has been amended or added to over time
- Who has access to protected data and why

The Senior Leadership Team, and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the Academy in accordance with this data protection policy and the GDPR.

Compliance with data protection legislation is the responsibility of all members of the Academy who process personal information.

Lawful basis for processing data under the GDPR article 6

- Consent
- Performance of a contract
- Legal obligation
- Protect vital interests
- Public interest task
- Legitimate interests

Lawful basis for processing special category data under the GDPR article 9

- Explicit consent
- Employment law
- Protect vital interest
- Not-for-profit body
- Manifestly made public
- Legal claims
- Substantial public interest
- Health purposes
- Public Health
- Archiving in the public interest

For further information on the lawful basis for processing please refer to the Academy's Data Protection Officer.

Consent

Wherever the lawful basis for processing an article 6 data does not fall into the performance of a contract, a legal obligation, protecting vital interests, a public interest task or legitimate interests; consent must be obtained from the individual.

Wherever the lawful basis for processing an article 9 special category data does not fall into employment law, protecting vital interest, not-for-profit body, manifestly made public, legal claim, substantial public interest, health purpose, public health or archiving in the public interest reason; explicit consent must be obtained from the individual.

In accordance with the GDPR, the Academy understands "consent" to mean that the data subject has been fully informed of the specific intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties and for “explicit consent” this must be in writing and signed. The individual must sign the consent document freely of their own accord. Consent cannot be inferred from non-response to a communication.

In most instances consent to process personal and sensitive data is obtained routinely by the Academy (e.g. when a student over the age of 13 signs a form or when a new member of staff signs a contract of employment). Any Academy forms (whether paper-based or web-based) that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain explicit consent if an individual's data are to be published on the Internet as such data can be accessed from all over the world. Therefore, not gaining consent could contravene the eighth data protection principle.

If an individual does not consent to certain types of processing (e.g. direct marketing), appropriate action must be taken to ensure that the processing does not take place.

If any member of the Academy is in any doubt about these matters, they should consult the Academy’s Data Protection Officer.

Data Protection (including GDPR) Principles

All processing of personal data must be done in accordance with the following data protection principles.

1. Personal data shall be processed fairly, lawfully and transparently. Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller and the data processor(s), the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Personal data shall be obtained for specific, explicit and lawful purposes and not processed in a manner incompatible with those purposes. Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held. Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

4. Personal data shall be accurate and, where necessary, kept up to date. Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by the Academy is accurate and up-to-date. Completion of an appropriate registration or application form etc. will be taken as an indication that the data contained therein is accurate. Individuals should notify the Academy of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Academy to ensure that any notification regarding change of circumstances is noted and acted upon and that inaccurate data is rectified without delay.

5. Personal data shall be kept in a form that permits identification, for the stated purpose, and only for as long as necessary and in accordance with the relevant retention schedule.

6. Personal data shall be processed in accordance with the rights of data subjects under the GDPR.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

8. Personal data must not be transferred outside of the European Economic Area (EEA) - the EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. [Members of the Academy should be particularly aware of this when publishing information on the Internet, which can be accessed from anywhere in the world. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.]

Rights of Data Subjects

Individuals have the following rights regarding data processing, and the data that are recorded about them:

- Right to be informed
- Right of access

Members of the Academy have the right to access any personal data which are held by the Academy in electronic format and in manual records which form part of a relevant filing system.

Any individual who wishes to exercise this right should apply in writing to the Academy's Data Protection Officer. Any such request will normally be complied with within 30 days of receipt of the written request.

The exceptions to the right of access are specific education data and child abuse data e.g.

  - If the disclosure is prohibited by law such as Education Health Care Plans (SEND regs)
  - If the request is made by a parent for details of an allegation that their child has been subject to/is at risk of child abuse
  - Information created by a teacher solely for their own use
  - Rights over data in an educational record not applying if 'serious harm test' is met i.e. subject access is likely to cause serious harm to physical or mental health of data subject or anyone else
  - Educational records

- Right to rectification
- Right to erase
- Right to restrict processing
- Right to data portability
- Right to object
- Rights on automated decision making and profiling

For further information on the rights of data subjects please refer to the Academy's Data Protection Officer.

Data Protection Impact Assessments (DPIA)

The Academy will carry out a DPIA when introducing new technologies and where the processing is likely to result in high risk to the rights and freedoms of individuals

Security of Data

All Academy staff are responsible for ensuring that any personal data which they hold on others are kept securely and that they are not disclosed to any unauthorised third party.

All personal data should be accessible only to those who need to use it. Academy staff should form a judgment based upon the sensitivity and value of the information in question, but always consider keeping personal data:

- In a lockable room with controlled access, or in a locked drawer or filing cabinet, or
- If computerised, password protected, or
- If kept on disks which are themselves kept securely.

All storage media must be appropriately secured in a safe environment that avoids physical risk, loss or electronic degradation.

Data must only be stored on Academy equipment (this includes computers and portable storage media). Private equipment (i.e. owned by users) must not be used.

When data is stored on any portable electronic system, USB stick or any other removable media the data must be encrypted and password protected, the device must be password protected and offer approved virus checking software. The data must be securely deleted from the device once it has been transferred or its use is complete.

Care should be taken to ensure that Computer screens are not visible except to authorised staff and that passwords are kept confidential. Screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel. User names and passwords should never be shared.

Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant computers should be wiped clean before disposal.

This policy also applies to staff and students who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and students should take particular care when processing personal data at home or in other locations outside of the Academy.

Users may not remove or copy sensitive or personal data from the Academy without permission and unless the media is encrypted and password protected and is transported securely for storage in a secure location.

Users must take particular care when working with data outside of the Academy that it cannot be accessed by other people and that they must have secure remote access.

For further details please refer to the Academy's ICT policy.

Disclosure of Data

The Academy must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, other members of staff/governors and in certain circumstances, the Police. All staff and students should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be deemed appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details or personal details to someone who wished to contact them regarding a non-work related matter. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Academy business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of the Academy concerned or to gain consent of the colleague to disclose their contact details to the requester.

This policy determines that personal data may be legitimately disclosed where one of the lawful basis for processing data applies.

When members of staff receive enquiries as to whether a named individual is a member of the Academy, the enquirer should be asked why the information is required. If consent for disclosure has not been given and the reason is not one detailed in the list of lawful basis for processing data, the member of staff should decline to comment. Even confirming whether or not an individual is a member of the Academy may constitute an unauthorised disclosure.

Unless consent has been obtained from the data subject, information should not be disclosed over the telephone. Instead, the enquirer should be asked to provide documentary evidence to support their request. Ideally a statement from the data subject consenting to disclosure to the third party should accompany the request. As an alternative to disclosing personal data, the Academy may offer to do one of the following:

- Pass a message to the data subject asking them to contact the enquirer;
- Accept a sealed envelope/incoming email message and attempt to forward it to the data subject. The enquirer should be informed that such action will be taken conditionally, i.e. "if the person is a member of the Academy" to avoid confirming their membership of, their presence in or their absence from the Academy.

Retention and Disposal of Data

The Academy discourages the retention of personal data for longer than they are required. Considerable amounts of data are collected on staff and students. However, once a member of staff or student has left the institution, it will not be necessary to retain all the information held on them indefinitely. Some data will be kept for longer periods than others.

Information relating to unsuccessful applicants in connection with recruitment to a post are kept only for a defined period after the interview date.

For further details on how long the Academy keeps various staff, student and applicant data, please refer to the Academy's retention schedules.

Disposal of Records

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion).

Publication of Academy Information

All members of the Academy should note that the Academy publishes a number of items that include personal data, and will continue to do so. These personal data are:

- Information published in the Academy Calendar
- Names of all members of Academy Committees
- Names, job titles and academic and/or professional qualifications of members of staff.
- Internal Telephone Directory.
- Information in prospectuses (including photographs), annual reports, newsletters, etc.
- Staff and student information on the Academy website (including photographs).

Explicit consent should be obtained from the data subject by the Academy whenever new personal data is published on the Academy website or in other media which could be accessed outside the EEA in accordance with the GDPR and the eighth data protection principle listed above.

It is also recognised that there might be occasions when a member of staff or student, requests that their personal details in some of these categories remain confidential or are restricted to internal access. All individuals have the right to object and restrict the publication of the above (and other) data. In such instances, the Academy should comply with the request and ensure that appropriate action is taken.

Use of CCTV

The Academy's use of CCTV is regulated by a separate Code of Practice and a separate Policy in accordance with the GDPR.

For reasons of personal security and to protect Academy premises and the property of staff and students, close circuit television cameras are in operation in certain locations. The presence of these cameras is not covert, although they may not always be obvious.

For further details please refer to the Academy's Closed Circuit Television (CCTV) Policy.