The Queen Katherine School Multi Academy Trust

DATA PROTECTION POLICY

This policy does not form part of any employee's contract of employment and we may amend it from time to time.

Committee:	MAT Board
Date of adoption:	May 2021
Date of next review:	May 2023

Document Control

The information in the table below details earlier versions of this document with a brief description of each review and how to distinguish amendments made since the previous version date (if any).

Version Number	Amended by:	Purpose	Approved by Trustees (date)
1		Original	
2		MAT Board review	May 2021
3		MAT Board review	

Data Protection Policy

1. RATIONALE

The Trust 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) 2018 and the Data Protection Act 2018.
The Trust needs to process certain information about its staff, students and other individuals with whom it has a relationship for various purposes such as, but not limited to:

- the recruitment and payment of staff
- the administration of programmes of study
- the recording of a student's progress
- agreeing awards
- collecting fees
- complying with legal obligations to funding bodies and government

To comply with various legal obligations, including the obligations imposed on it by the GDPR/DPA, The Trust must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully.

2. ASSOCIATED TRUST POLICIES

- Overarching Safeguarding Statement
- Child Protection Policy
- E-Safety Policy and Acceptable Use Agreements
- CCTV Procedures
- Health and Safety Policy
- Procedures for Using students Images
- Whole School Behaviour Policy
- Code of Conduct Policy
- IRMS Toolkit (Information Records Management for Schools)

3. COMPLIANCE

This policy applies to all members, governors/trustees, staff and students of The Trust. Any breach of this policy, or of the Act itself will be considered an offence and the school's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with The Trust, and who have access to personal information, will be expected to read and comply with this policy. It is expected that departments or individuals who are responsible for dealing with external bodies will take the responsibility for ensuring that such bodies sign a contract which among other things will include an agreement to abide by this policy.

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

The Information Commissioner's Office (ICO) www.ico.gov.uk gives further detailed guidance.

4. THE GENERAL DATA PROTECTION REGULATION 2018/DATA PROTECTION ACT 2018

The GDPR/DPA regulates the processing of personal data, and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request' (sample held at Appendix A). Personal

data is information relating to an individual and may be in hard or soft copy (paper/ manual files; electronic records; photographs; CCTV images), and may include facts or opinions about a person.

5. RESPONSIBILITIES UNDER THE GENERAL DATA PROTECTION REGULATION/DPA

The individual school will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data.

The Headteacher of each school is responsible for all day-to-day data protection matters, and he/she will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the school.

The school is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Compliance with the legislation is the responsibility of all staff of the Trust who process personal information.

Individuals who provide personal data to the Trust are responsible for ensuring that the information is accurate and up-to-date.

6. DEFINITIONS

Data Controller:	Any individual or organisation who controls personal data.
Data Processor:	The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Data Protection Officer:	Monitors compliance with this regulation and cooperates with the information commissioner's office.
Personal Data*:*	Data which relates to a living individual who can be identified. Addresses and telephone numbers are particularly vulnerable to abuse, but so can names and photographs be, if published in the press, Internet or media.
Sensitive Personal Data*:*	Personal data relating to an individual's race or ethnic origin, political opinions, religious beliefs, physical/mental health, trade union membership, sexual life or criminal activities.
Relevant Filing System:	Also known as manual records i.e. a set of records which are organised by reference to the individual/their criteria and are structured in such a way as to make specific information readily accessible e.g. personnel records, microfiches.
Data Subject*:*	An individual who is the subject of the personal data, for example, employees, students, claimants etc.
Processing*:*	Obtaining, recording or holding data or carrying out any operation on the data including organising, adapting, altering, retrieving, consulting, using, disclosing, disseminating, aligning, blocking, erasing or destroying the data.
***Accessible Records*:**	Any records which are kept by the Trust as part of a statutory duty, e.g. student records.
Parent:	Has the meaning given in the Education Act 1996, and includes any person having parental responsibility or care of a child.

7. DATA PROTECTION PRINCIPLES

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. In order to comply with its obligations, The Trust undertakes to:

7.1 Process personal data fairly and lawfully

The Trust will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller; the purposes of the processing; any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

7.2 Process the data for the specific and lawful purpose for which it collected that data, and not further process the data in a manner incompatible with this purpose

The Trust will ensure that the reason for which it collected the data originally is the only reason for which it processes those data, unless the individual has been or is informed of any additional processing.

7.3 Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed

The Trust will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data are given by individuals, they will be destroyed.

7.4 Keep personal data accurate and, where necessary, up to date

The Trust will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the school if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the school to ensure that any notification regarding the change is noted and acted on.

7.5 Only keep personal data for as long as is necessary

The Trust undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means The Trust will undertake a regular review of the information held and implement a regular weeding process.

The Trust will dispose of any personal data in a way that protects the rights and privacy of the individual concerned. See also Section 16.

7.6 Process personal data in accordance with the rights of the data subject under the legislation

Individuals have various rights under the legislation including:

- a right to be told the nature of the information the Trust holds and any parties to whom this may be disclosed;
- a right to prevent processing likely to cause damage or distress;
- a right to prevent processing for purposes of direct marketing;
- a right to be informed about the mechanics of any automated decision making process that will significantly affect them;
- a right not to have significant decisions that will affect them taken solely by automated process;
- a right to sue for compensation if they suffer damage by any contravention of the legislation;
- a right to take action to rectify, block, erase, or destroy inaccurate data;
- a right to request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened;
- a right to receive personal data that he or she has given to the controller and have it transmitted to another controller;

The Trust will only process personal data in accordance with individuals' rights.

7.7 Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data

All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

The Trust will ensure that all personal data is accessible only to those who have a valid reason for using it.

The Trust will have in place appropriate security measures e.g.

- ensuring that hard copy personal data is kept in lockable filing cabinets/ cupboards with controlled access;
- keeping all personal data in a lockable room with key-controlled access;
- password protecting personal data held electronically;
- archiving personal data on disks which are then kept securely (lockable cabinet);
- placing any PCs or terminals, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.

In addition, The Trust will put in place appropriate measures for the deletion of personal data – manual records will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work. Hard drives of redundant PCs will be wiped clean before disposal, or if that is not possible, destroyed physically.

This policy also applies to staff and students who process personal data 'off-site', e.g. when working at home, and in such circumstances additional care must be taken regarding the security of the data.

7.8 Ensure that no personal data is transferred to a country or a territory outside the European Economic Area unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The Trust will not transfer data to such territories without the explicit consent of the individual.

This also applies to publishing information on the Internet – because transfer of data can include placing data on a website that can be accessed from outside the EEA – so The Trust will always seek consent before placing any personal data (including photographs) on its website.

If the Trust collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

8. CONSENT AS A BASIS FOR PROCESSING

Where processing is based on consent, the Trust shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
Consent is especially important when schools are processing any sensitive data, as defined by the legislation.

The Trust understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement (e.g. via signing a form), whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing.

The Trust will ensure that any forms used to gather data on an individual will contain a statement (Privacy Notice) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

The Trust will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place. **A copy of the student and workforce Privacy notices are posted on the home pages of all Schools websites within the Trust.**

8.1 Lawful Processing

Under the "Lawfulness of Processing" requirements in the GDPR, the Trust will inform staff and separately parents/carers of all students of the data they hold on the staff member or student, the purposes for which the data is held and the third parties (e.g. LA, DfE, QCA etc.) to whom it may be passed. This Privacy Notice will be passed to staff when they join the school and parents/carers through *(to be inserted – schools might choose to use the Prospectus, newsletters, reports or a specific letter/communication)*. Parents/carers of young people who are new to the school will be provided with the Privacy Notice through *(to be inserted – as above)*.

Privacy Notices can be found at the home page of each School website within the Trust.

9. SUBJECT ACCESS RIGHTS (SARS)

The GDPR extends to all data subjects a right of access to their own personal data. In order to ensure that people receive only information about themselves it is essential that a formal system of requests is in place. Where a request for subject access is received from a student, the school's policy is that:

- Requests from student will be processed as any subject access request as outlined below and the copy will be given directly to the student.
- Requests from students who do not appear to understand the nature of the request will be referred to their parents or carers.
- Requests from parents in respect of their own child will normally be processed as requests made on behalf of the data subject (the child) and the copy will be sent in a sealed envelope to the requesting parent. The Trust will seek consent from the child if the child is 13 years old or over and has the ability to understand their rights.
- The information is provided free but subsequent copies would be charged at a reasonable amount to cover admin costs.
- Any requests that are manifestly unfounded or excessive may be refused.

9.1 Processing Subject Access Requests

Requests for access must be made in writing.

Students, parents or staff may ask for a Data Subject Access form (see Appendix A), available from the School Office. Completed forms should be submitted to the nominated person.. Provided that there is sufficient information to process the request, an entry will be made in the Subject Access log book, showing the date of receipt, the data subject's name, the name and address of requester *(if different)*, the type of data required (e.g. Student Record, Personnel Record), and the planned date of supplying the information (normally not more than 30 days from the request date). Should more information be required to establish either the identity of the data subject (or agent) or the type of data requested, the date of entry in the log will be the date on which sufficient information has been provided.

10. AUTHORISED DISCLOSURES

The Trust will, in general, only disclose data about individuals with their consent. However there are circumstances under which the Trust's authorised officers may need to disclose data without explicit consent for that occasion.

These circumstances are strictly limited to:

- Student data disclosed to authorised recipients related to education and administration necessary for the Trust to perform its statutory duties and obligations.
- Student data disclosed to authorised recipients in respect of the child's health, safety and welfare.

- Student data disclosed to parents in respect of their child's progress, achievements, attendance, attitude or general demeanour within or in the vicinity of the school where the child is not mature enough to exercise its own rights.
- Staff data disclosed to relevant authorities e.g. in respect of payroll and administrative matters.
- Unavoidable disclosures, for example to an engineer during maintenance of the computer system. In such circumstances the engineer would be required to sign a form promising not to disclose the data outside the Trust. Officers and IT personnel writing on behalf of the LA are IT liaison/data processing officers, for example in the LA, are contractually bound not to disclose personal data.
- Only authorised and trained staff are allowed to make external disclosures of personal data. Data used within the Trust by administrative staff, teachers and welfare officers will only be made available where the person requesting the information is a professional legitimately working within the Trust who **need to know** the information in order to do their work. The Trust will not disclose anything on students' records which would be likely to cause serious harm to their physical or mental health or that of anyone else – including anything where suggests that they are, or have been, either the subject of or at risk of child abuse.

10.1 Legal Disclosure

A **"legal disclosure"** is the release of personal information from the computer to someone who requires the information to do his or her job within or for the Trust, provided that the purpose of that information has been registered.

10.2 Illegal Disclosure

An **"illegal disclosure"** is the release of information to someone who does not need it, or has no right to it, or one which falls outside the Trust's registered purposes.

11. PUBLICATION OF TRUST INFORMATION

The Trust publishes various items which will include some personal data, e.g.

- internal telephone directory
- event information
- staff information
- lists of students

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted to internal school access only. Therefore it is The Trust's policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Staff records appertaining to individual staff will remain of a confidential nature between the Headteacher and the member of staff and, where appropriate, the Trust HR Manager and/or line manager.

11.1 Email

It is the policy of The Trust to ensure that senders and recipients of email are made aware that under the GDPR, and Freedom of Information legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the Trust's email.

Under the Regulation of Investigatory Powers Act 2000 and Lawful Business Practice Regulations, any email sent to or from the Trust may be accessed by someone other than the recipient for system management and security purposes.

11.2 CCTV

There are some CCTV systems operating within The Trust for the purpose of protecting staff, students, visitors and property. The Trust will only process any personal data obtained by the CCTV system in a

manner which ensures compliance with the legislation.

For detailed guidance on CCTV see the ICO Code of Practice on CCTV which can be accessed at www.ico.gov.uk .

11.3 Images/Photographs

Information regarding our policy for the use of students' images and model Parental Consent forms can be found in:

Voluntary Aided and Foundation Schools and Academies - KAHSC General Safety Series G21

12. DATA INTEGRITY

The Trust undertakes to ensure data integrity by the following methods:

12.1 Data Accuracy

Data held will be as accurate and up to date as is reasonably possible. If a data subject informs the Trust of a change of circumstances their computer record will be updated as soon as is practicable. A printout of their data record will be provided to data subjects every twelve months so they can check its accuracy and make any amendments.

Where a data subject challenges the accuracy of their data, the Trust will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Board for their judgment. If the problem cannot be resolved at this stage, either side may seek independent arbitration. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

12.2 Data Adequacy and Relevance

Data held about people will be adequate, relevant and not excessive in relation to the purpose for which the data is being held. In order to ensure compliance with this principle, the Trust will check records regularly for missing, irrelevant or seemingly excessive information and may contact data subjects to verify certain items of data.

12.3 Length of Time

Data held about individuals will not be kept for longer than necessary for the purposes registered. It is the duty of **the Data Protection Responsible Person** to ensure that obsolete data are properly erased. See also Section 16.

13. IDENTIFICATION OF DATA

The Trust will ensure that all staff, contractors working for it, and delivery partners, comply with restrictions applying to the access to, handling and storage of data classified as Protect, Restricted or higher.

The Trust recognises that under Article 15 of the GDPR, data subjects have a number of rights in connection with their personal data, the main one being the right of access. Procedures are in place to deal with Subject Access Requests i.e. a written request to see all or a part of the personal data held by the data controller in connection with the data subject (details can be found in Section 10). Data subjects have the right to know: if the data controller holds personal data about them; a description of that data; the purpose for which the data is processed; the sources of that data; to whom the data may be disclosed; and a copy of all the personal data

that is held about them. Under certain circumstances the data subject can also exercise rights in connection with the rectification; blocking; erasure; objection; restriction and destruction of data.

14. DATA AND COMPUTER SECURITY

The Trust undertakes to ensure security of personal data by the following general methods (precise details cannot, of course, be revealed):

14.1 Physical Security

Appropriate building security measures are in place, such as alarms, window locks, deadlocks and computer rooms kept locked. Only authorised persons are allowed in the computer room. Disks, tapes and printouts are locked away securely when not in use. Visitors to the individual academy schools are required to sign in and out, to wear identification badges whilst in the school and are, where appropriate, accompanied.

14.2 Logical Security

- Security software is installed on all computers containing personal data.
- The Trust will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them.
- All users will be given secure user names and strong passwords which must be changed regularly. User names and passwords must never be shared.
- Personal data may only be accessed on machines that are securely password protected. Any device that can be used to access data must be locked if left (even for very short periods) and set to auto lock if not used for five minutes.
- All storage media must be stored in an appropriately secure and safe environment that avoids physical risk, loss or electronic degradation.
- Personal data can only be stored on Trust equipment (this includes computers and portable storage media). Private equipment (i.e. owned by the users) must not be used.
- When personal data is stored on any portable computer system, USB stick or any other removable media:

    - the data must be encrypted and password protected;
    - the device must be password protected (many memory sticks/cards and other mobile devices cannot be password protected);
    - the device must offer approved virus and malware checking software;
    - the data must be securely deleted from the device, in line with Trust policy (below) once it has been transferred or its use is complete.

    Under no circumstances should any data be downloaded from the school's network in order to remove from the school's premises as each staff member is provided with remote access.

- The Trust has clear policy and procedures for the automatic backing up, accessing and restoring all data held on Trust systems, including off-site backups.

14.3 Procedural Security

In order to be given authorised access to the computer, staff will have to undergo checks and will sign a confidentiality agreement (acceptable use statement). All staff are trained in their Data Protection obligations and their knowledge updated as necessary. Computer printouts as well as source documents are shredded before disposal.

Further information can be found in the Trust E-Safety Policy.

Overall security policy for data is determined by the Board of the Trust and is monitored and reviewed regularly, especially if a security loophole or breach becomes apparent. The Trust's security policy is kept in a safe place at all times.

Any queries or concerns about security of data in the Trust should in the first instance be referred to **the Data Protection Officer at dpo@walney.cumbria.sch.uk**

subject to claims for damages from persons who believe that they have been harmed as a result of inaccuracy, unauthorised use or disclosure of their data. A deliberate breach of this Data Protection Policy will be treated as disciplinary matter, and serious breaches could lead to dismissal.

15. SECURE TRANSFER OF DATA AND ACCESS OUT OF SCHOOL

The Trust recognises that personal data may be accessed by users out of school or other agencies. In these circumstances:

- Under no circumstances should any data be downloaded from the school's network in order to remove from the school's premises as each staff member is provided with remote access.
- When data is required by an authorised user from outside the Trust premises (for example, by a teacher or student working from their home or a contractor) they must have secure remote access to the management information system (MIS) or learning platform.
- Particular care should be taken if data is taken or transferred to another country, particularly outside Europe. (NB. to carry encrypted material is illegal in some countries)

16. DISPOSAL OF DATA

The Trust will comply with the requirements for the safe destruction of personal data when it is no longer required.

The disposal of protected data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten and other media must be shredded, incinerated or otherwise disintegrated for data.

17. TRAINING & AWARENESS

All staff will receive data handling awareness/data protection training and will be made aware of their responsibilities, as described in this policy through:

- Induction training for new staff;
- Staff meetings/briefings/Inset;
- Day to day support and guidance from the Responsible Person.

18. ENQUIRIES

Information about the Trust Data Protection Policy is available from **the Headteacher**. General information about the General Data Protection Regulation can be obtained from the Data Protection Officer(DPO) or the Information Commissioners Office http://www.ico.gov.uk/.

A copy of this policy will be issued to all employees and covered in new staff Induction training. It will be reviewed annually, added to, or modified from time to time and may be supplemented in appropriate cases by further statements and procedures relating to the work of the particular groups of workers.

APPENDIX A

ACCESS TO PERSONAL DATA REQUEST
(Subject Access Request – SARS)
General Data Protection Regulation 2018 Article 15

Enquirer's Surname		**Enquirer's Forenames**	
Enquirer's Address			
Enquirer's Postcode:			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			**YES / NO**
If NO,			
Do you have parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			**YES / NO**
If YES,			
Name of child or children about whose personal data records you are enquiring:	_____ _____ _____ _____		
Description of Concern / Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please despatch Reply to: *(if different from enquirer's details as stated on this form)*

Name

Address

Postcode

DATA SUBJECT DECLARATION

I request that the Trust search its records based on the information supplied above under Article 15 of the General Data Protection Regulation 2018 and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the Trust.

I agree that the reply period will commence when I have supplied sufficient information to enable the Trust to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and
Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _

Name of "Data Subject" (or Subject's Parent) (PRINTED) _

Dated _____