Four Cs
Multi-Academy Trust

GENERAL DATA PROTECTION REGULATIONS (GDPR) POLICY

Presented to:

Full Trustees Meeting
4 July 2019

Date approved:[1]	29 March 2018 (for one year as a working draft)
Date reviewed:[2]	4 July 2019
Date of next review:[3]	Summer 2022

[1] This is the date the policy was approved by the meeting
[2] This is the date the policy was reviewed prior to its approval above
[3] This is the date as set by the policy review clause or the date approved plus two years

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

Note that in the context of the Protection of Freedoms Act 2012, a "child" means a person under the age of 18.

1.0 General Data Protection Regulations (GDPR)

1.1 The Four Cs Trust, and its respective schools, collects and uses personal information about staff, student/pupils, parents and other individuals who come into contact with the Trust and its schools. This information is gathered in order to enable it to provide education and other associated functions.

1.2 Information includes contact details, National Curriculum assessment results, attendance information, personal characteristics such as ethnic group, special educational needs and any relevant medical information.

1.3 In addition, there may be a legal requirement to collect and use information to ensure that the Trust complies with its statutory obligations. From time to time Trust schools are legally required to pass on some of this data to others. This includes the Local Authority (LA), to other schools to which a student/pupil is transferring, to the Department for Education (DfE) and to the Qualifications and Curriculum Authority (QCA) which is responsible for the National Curriculum and associated assessment arrangements.

1.4 Local Authorities use information about student/pupils to carry out specific functions for which it is responsible. For example, the assessing of any Special Educational Needs the student/pupil may have. It also uses the information to gather statistics to make essential decisions on, for example, funding schools, and to assess the performance of schools and set targets for them. It uses the statistics in such a way that individual student/pupils cannot be identified.

1.5 The Trust has a duty to be registered, as Data Controller, with the Information Commissioner's Office (ICO), detailing the information held and its use. These details are then available on the ICO's website. The Trust has a duty to issue a Privacy Notice to all students/pupils/parents/staff (see Appendix 1), this summarises the information held, why it is held and the other parties to whom it may be passed on.

2.0 Purpose

2.1 This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations (GDPR). It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

3.0 Roles and Responsibilities

This policy applies to **all staff** employed by Trust schools, and to external organisations or individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action.

3.1 <u>Trustees</u>

The Trustees have overall responsibility for ensuring that Trust schools comply with all relevant data protection obligations.

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

3.2 Data Protection Officer

The Data Protection Officer (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

The DPO will support the Trust schools and provide staff with a guidance booklet.

The DPO will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the Trust their advice and recommendations on data protection issues within the Trust schools.

3.3 Headteacher

The Headteacher of each Trust school acts as the representative of the data controller on a day-to-day basis.

3.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing their respective Trust school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
    - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
    - If there has been a data breach
    - Whenever they are engaging in a new activity that may affect the privacy rights of individuals
    - If they need help with any contracts or sharing personal data with third parties

4.0 What is Personal Information?

4.1 Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

5.0 General Data Protection Principles

5.1 The General Data Protection Regulations establish 6 enforceable principles that must be adhered to at all times. Personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which the data is processed
- Accurate and kept up to date
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed
- Processed in a way that ensures appropriate security of personal data.

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

6.0 General Statement

6.1 The Trust is committed to maintaining the above principles at all times. Therefore, the Trust will:

- Inform individuals why the information is being collected, when it is collected and the legal basis for collecting it
- Inform individuals via Privacy Notices how information is shared, and why and with whom
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure Trust staff are aware of and understand our policies and procedures

7.0 Individual Rights

7.1 Under GDPR, individuals have the following rights:

- The right to erasure
- The right to restrict processing – unless there is a legitimate legal basis for continuing to do so
- The right to data portability
- The right to object – unless there is an overriding legitimate reason to continue
- Rights in relation to automated decision-making or profiling

8.0 Collecting personal data

8.1 <u>Lawfulness, fairness and transparency</u>

Trust schools will only process personal data where there are one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that a Trust school can **fulfil a contract** with the individual, or the individual has asked a Trust school to take specific steps before entering into a contract
- The data needs to be processed so that a Trust school can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual eg to protect someone's life
- The data needs to be processed so that a Trust school, as a public authority, can perform a task **in the public interest,** and carry out its official functions
- The data needs to be processed for the **legitimate interests** of the Trust school or a third party (provided the individual's rights and freedoms are not overridden)
- The individual (or their parent/carer when appropriate in the case of a student/pupil) has freely given clear **consent**

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

8.2 Limitation, minimisation and accuracy

- Trust schools will only collect personal data for specified, explicit and legitimate reasons. A Trust school will explain these reasons to the individuals when data is first collected in the form of Privacy Notices
- If a Trust school wants to use personal data for reasons other than those given when it is first obtained, individuals concerned will be informed before it does so, and seek consent where necessary
- Staff must only process personal data where it is necessary in order to do their jobs
- When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

9.0 Sharing personal data

Trust schools will not normally share personal data with anyone else, but may do so where:

- There is an issue with a student/pupil or parent/carer that puts the safety of our staff at risk
- There is a need to liaise with other agencies –consent will be sought as necessary before doing this
- Suppliers or contractors need data to enable services to be provided to staff and student/pupils – for example, IT companies. When doing this, Trust schools will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data that is shared
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with the Trust school.

9.1 Trust schools will also share personal data with law enforcement and government bodies where it is legally required to do so, including for:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

9.2 Trust schools may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any student/pupils or staff.

9.3 Where a Trust school transfers personal data to a country or territory outside the European Economic Area, it will be done so in accordance with data protection law.

10.0 Subject Access Requests

10.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the school holds about them. This must be made in writing and must include the following:

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

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

10.2 Employees who receive a written request should forward it initially to their respective Headteacher who will in turn inform the Trust's Data Protection Officer. The response time for subject access requests, once officially received, is one calendar month. Although no charges are made for information provided, Trust schools reserve the right to consider charging for multiple, repetitious requests from the same data subject if it is felt appropriate.

10.3 When / if receiving telephone enquiries, a Trust school will only disclose personal data held on their systems if the caller's identity is checked and proof of relationship to child, if applicable, is established.

11.0 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request, or have given their consent.

11.1 Primary schools:
Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of student/pupils at a Trust school may be granted without the express permission of the student/pupil. This is not a rule and a student/pupil's ability to understand their rights will always be judged on a case-by-case basis.

11.2 Secondary schools:
Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of student/pupils at a Trust school may not be granted without the express permission of the student/pupil. This is not a rule and a student/pupil's ability to understand their rights will always be judged on a case-by-case basis.

12.0 Responding to subject access requests

12.1 When responding to requests, a Trust school:

- May ask the individual to provide 2 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
- Where a request is complex or numerous a Trust school may tell the individual that it will comply within 3 months of receipt of the request. The Trust school will inform the individual of this within one month, and explain why the extension is necessary

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

12.2 A Trust school will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student/pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child

12.3 If the request is unfounded or excessive, a Trust school may refuse to act on it, or charge a reasonable fee which takes into account administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information. When a Trust school deems it necessary to ignore a request, it will ensure that the DPO is in agreement before notifying the individual. When a Trust school refuses a request, it will tell the individual why, and tell them they have the right to complain to the ICO.

13.0 Consent

13.1 Where data is subject to active consent by the data subject, this consent can be revoked at any time in writing.

14.0 Biometric Recognition Systems

14.1 Where a Trust school uses student/pupils' biometric data as part of an automated biometric recognition system (for example, student/pupils use finger prints to receive school dinners instead of paying with cash), it will comply with the requirements of the Protection of Freedoms Act 2012.

14.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The Trust school will get written consent from at least one parent/carer before any biometric data is taken from their child and first processed.

14.3 Parents/carers and student/pupils have the right to choose not to use the school's biometric system(s). A Trust school will provide alternative means of accessing the relevant services for those student/pupils.

14.4 Parents/carers and student/pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the Trust school will make sure that any relevant data already captured is deleted.

14.5 As required by law, if a student/pupil refuses to participate in, or continue to participate in, the processing of their biometric data, the Trust school will not process that data irrespective of any consent given by the student/pupil's parent/carers.

14.6 Where staff members or other adults use the school's biometric system(s), the Trust school will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

15.0 CCTV (where installed)

Trust schools use CCTV in various locations around the school site to ensure it remains safe. The Trust school will adhere to the ICO's code of practice for the use of CCTV. See separate Security Policy for further information.

16.0 Photographs and videos

As part of school activities, a Trust school may take photographs and record images of individuals within the school.

16.1 Primary schools
The Trust school obtains written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials.

16.2 Secondary schools
The Trust school obtains written consent from parents/carers, or student/pupils aged 18 and over, for photographs and videos to be taken of student/pupils for communication, marketing and promotional materials.

16.3 Uses may also include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on a school website or social media pages

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

16.5 When using photographs and videos in this way the Trust school will not accompany them with any other personal information about the child, to ensure they cannot be identified.

17.0 Data protection by design and default

17.1 The Trust will put measures in place to show that it has integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law
- Completing Data Protection Impact Assessments where the processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; it will also keep a record of attendance
- Conducting reviews and audits to test our privacy measures and make sure it is compliant

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

18.0 Data security and storage of records

18.1 Trust schools will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage.

18.2 In particular:

- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Encryption software is used to protect laptops
- Staff, student/pupils or Trustees/Governors should not store personal information on their personal devices
- Where a Trust school needs to share personal data with a third party, it will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected

19.0 Retention and Disposal of Data

19.1 Trust schools will hold student/pupil data for no longer than is necessary for the purpose or purposes it was collected. Reasonable steps will be taken to destroy, or erase from the systems, all data which is no longer required.

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

19.3 Trust schools will shred or incinerate paper-based records, and overwrite or delete electronic files. A third party may be used to safely dispose of records on the school's behalf. If it does so, it will require the third party to provide sufficient guarantees that it complies with data protection law.

20.0 Data Breaches

20.1 A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

20.2 Personal data breaches could include:

- access by an unauthorised third party
- deliberate or accidental action (or inaction) by a controller or processor
- sending personal data to an incorrect recipient
- computing devices containing personal data being lost or stolen
- alteration of personal data without permission
- loss of availability of personal data.

20.3 When a personal data breach has occurred, the DPO will need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it is a risk, then the DPO will report to the ICO.

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

20.4 Trust schools will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the Trust will follow the procedure set out. When appropriate, the Trust will report the data breach to the ICO within 72 hours through the DPO.

21.0 Training

21.1 All staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or processes make it necessary.

22.0 Compliance

22.1 The Trust is committed at the highest level to putting relevant policies and procedures in place to demonstrate compliance. These involve the following:

- Ensuring appropriate technical and organisational measures are in place
- Keeping records on data processing activities (eg records of data shared with which organisations)
- Undertaking Data Protection Impact Assessments eg when considering implementation of new systems
- Ensuring third party suppliers (for example parent payment platforms) are GDPR compliant, and that legally-binding contracts with any company processing personal data are in place.

23.0 Data Protection Impact Assessments (DPIA)

23.1 A DPIA should be carried out when:
- using new technologies; and
- the processing is likely to result in a high risk to the rights and freedoms of individuals.

23.2 The three primary conditions identified in the GDPR are:
- A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person
- Processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences
- Systematic monitoring of a publicly accessible area on a large scale.

23.3 When conducting a DPIA it must contain:
- A description of the processing operations and the purposes, including, where applicable, the legitimate interests pursued by the controller
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An assessment of the risks to individuals
- The measures in place to address risk, including security and to demonstrate compliance.

23.4 The DPIA should be driven by people with appropriate expertise and knowledge of the project in question. In addition, the organisation should seek the DPO's advice as a part of the process.

23.5 Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

24.0 Contacts

24.1 If you have any enquires in relation to this policy, please contact the Trust's Data Protection Officer who will also act as the contact point for any subject access requests (this information is available in the Trust's Privacy Notices). Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

25.0 Complaints

25.1 Complaints will be dealt with in accordance with the Trust's Complaints Policy. Complaints relating to information handling or which are not appropriate to be dealt with through the Trust's Complaints procedure may be referred to the Information Commissioner (the statutory regulator).

26.0 Review

26.1 The Trust Board will review this policy in line with the procedure for policy review.

Date for Review

If no other reason for review, this policy will be reviewed every three years by the Trustees with the next review being Spring 2022.

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust

Appendix 1 – Privacy Notices (Learner and Workforce)

See separate documents

- Headteacher also means Head of College and Principal
- School also means College, Academy or Academies
- References to School are taken to mean any school within the Four Cs Multi-Academy Trust