The Four Stones Multi Academy Trust
Data protection policy

Version Control
Policy author: Ruth Allen
Policy approved by: Finance, Audit and Risk Committee
Next policy review date: Autumn 2021

Version	Date	Details
1.0	9th Dec 2019	Re-written so that there is one policy for The Four Stones Multi Academy Trust
2.0	23rd June 2020	General review and change of data protection officer for Haybridge High School
3.0	25th Nov 2020	Updated to show the creation of a data protection officer for the MAT, the addition of a data protection representative in each school and include The De Montfort School

Contents

1. Aims

The Four Stones Multi Academy Trust (MAT) aims to ensure that all personal data collected about staff, students, parents/carers, members, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018). This policy applies to all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005, which gives parents the right of access to their child's educational record. In addition, this policy complies with our funding agreement and articles of association.

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, individual. This may include the individual's: ▪ Name (including initials) ▪ Identification number ▪ Location data ▪ Online identifier, such as a username It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.
Special categories of personal data	Personal data which is more sensitive and so needs more protection, including information about an individual's: ▪ Racial or ethnic origin ▪ Political opinions ▪ Religious or philosophical beliefs ▪ Trade union membership ▪ Genetics ▪ Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes ▪ Health – physical or mental ▪ Sex life or sexual orientation
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data subject	The identified or identifiable individual whose personal data is held or processed.
Data controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

4. The data controller

The MAT processes personal data relating to parents/carers, students, staff, members, trustees, governors, visitors and others, and therefore is a data controller. The MAT is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

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

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that our schools comply with all relevant data protection obligations.

5.2 Data protection officer (DPO)
The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable. They will provide an annual report of their activities directly to the local governing board and, where relevant, report to the board their advice and recommendations on school data protection issues. The DPO is the first point of contact for the ICO. Full details of the DPO's responsibilities are set out in their job description. Please see appendix 1 for the relevant contact details.

5.3 Data protection representative (DPR)
Each school in the MAT has a data protection representative (DPR). The role of the DPR is to support the MAT's DPO, oversee the implementation of this policy and other related policies in their school, monitor their school's compliance with data protection law and provide staff training in line with the DPO's guidance. The DPR is also the first point of contact for individuals whose data the school processes. Full details of the DPR's responsibilities are set out in their job description. Please see appendix 1 for the relevant contact details.

5.4 CEO/Executive Headteacher
The CEO/executive headteacher is responsible for ensuring that the data protection policy and guidelines are being adhered to.

5.5 Associate Headteachers
The associate headteachers of the individual schools act as the data controllers on a day-to-day basis.

5.6 Information Asset Owners
The MAT has also identified Information Asset Owners (IAOs) for the various types of data being held in each school (e.g. student/ staff information, assessment data etc). These IAOs will manage and address risks to the information and understand what information is held and for what purpose, how information has been amended or added to over time, and who has access to protected data and why. They will ensure that information in their care is protected by an appropriate level of security, through, for example, password protection or where necessary, encryption. Please see appendix 2 for the current appointees.

5.7 All staff
Staff are responsible for:
- Collecting, storing and processing any personal data in accordance with this policy
- Informing the MAT of any changes to their personal data, such as a change of address
- Contacting the DPR 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

5.8 Parents/carers
All parents/carers are responsible for:
- checking that any information they provide to the relevant school within the MAT is accurate and up to date
- informing the relevant school within the MAT of any changes to information which they have provided, e.g. changes of address, telephone numbers
- informing the relevant school within the MAT of any errors in the information that the school holds about them

The MAT cannot be held responsible for any errors of which it has not been informed

6. Data protection principles
The GDPR is based on data protection principles that the MAT must comply with. The principles say that 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 to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

This policy sets out how the MAT aims to comply with these principles.

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the individual schools within the MAT can **fulfil a contract** with the individual, or the individual has asked the school to take specific steps before entering into a contract
- The data needs to be processed so that the individual schools within the MAT can **comply with a legal obligation**
- The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life
- The data needs to be processed so that the schools within the MAT, 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 individual schools within the MAT 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) has freely given clear **consent**

For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR and Data Protection Act 2018.

If we offer online services to students and we intend to rely on consent as a basis for processing, we will get parental consent where the student is under 13 (except for online counselling and preventive services).

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

7.2 Limitation, minimisation and accuracy

We will only collect personal data for specified, explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do 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. This will be done in accordance with the Information and Records Management Society's toolkit for schools. See appendix 4 for further information on records retention and management.

8. Sharing personal data

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

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we 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 we share
  - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are 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 our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our students or staff.

Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

9. Subject access requests and other rights of individuals

9.1 Subject access requests

Individuals have a right to make a 'subject access request' to gain access to personal information that the MAT holds about them. This includes:

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The purposes of the data processing
- The categories of personal data concerned
- Who the data has been, or will be, shared with
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- The source of the data, if not the individual
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual

If staff receive a subject access request they must immediately forward it to the relevant DPR. Please see appendix 5 for further information on how to make a subject access request.

9.2 Children and subject access requests

Personal data about a child belongs to that child, and not the child's parents/carers. For a parent/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.

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/carers of students at our individual schools may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

When responding to requests, we:

- 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 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the student 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

If the request is unfounded or excessive, we 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 we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

Please see appendix 5 for further information on how to make a subject access request.

9.4 Other data protection rights of the individual

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress

- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

Individuals should submit any request to exercise these rights to the relevant DPR. If staff receive such a request, they must immediately forward it to the relevant DPR.

10. Parental requests to see the educational record

Under data protection legislation, parents/carers and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, please contact: King Charles I School on 01562 512880 or via email at office@kingcharles1.worcs.sch.uk; Haybridge High School on 01562 886213 or via email at office@haybridge.worcs.sch.uk; or The De Montfort School on 01386 442060 or via email at office@tdms.worcs.sch.uk

Under data protection law, individuals have certain rights regarding how their personal data is used and kept safe, including the right to:

- Object to the use of personal data if it would cause, or is causing, damage or distress
- Prevent it being used to send direct marketing
- Object to decisions being taken by automated means (by a computer or machine, rather than by a person)
- In certain circumstances, have inaccurate personal data corrected, deleted or destroyed, or restrict processing
- Claim compensation for damages caused by a breach of the data protection regulations

To exercise any of these rights, please contact the relevant DPR (see appendix 1).

11. Biometric recognition systems

Where we use students' biometric data as part of an automated biometric recognition system (for example, students use finger prints to receive school dinners instead of paying with cash) we will comply with the requirements of the Protection of Freedoms Act 2012.

Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The individual schools will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

Parents/carers and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those students. For example, students can pay for school dinners using a pin number instead.

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

As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the student's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), we 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 MAT will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around our school sites to ensure they remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

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.

Any enquiries about the CCTV system should be directed to Jessica Bushell (the MAT's chief operating officer) on jbushell@thefourstonesmat.co.uk or 01562 512880.

13. Photographs and videos

As part of our individual schools' activities, we may take photographs and record images of individuals within our schools. We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and student. Where we don't need parental consent, we will clearly explain to the student how the photograph and/or video will be used. Uses may include:

- For the profile picture on the school's information management system
- For GCSE and A Level examination submissions
- Performing arts including dance and movement, concerts and drama performances
- Sports days and sports fixtures and the use of photographic equipment by parents/carers
- Media, including newspapers and television
- Displays in school.
- The school's website-e.g. prospectus and other publications.
- The school's twitter account
- Staff training and professional development activities
- Site security CCTV videos

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.

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

See our 'Photographic Images of Children' policy for more information on our use of photographs and videos.

14. Data protection by design and default

We will put measures in place to show that we have 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 (see section 6)
- Completing privacy impact assessments where the MAT's or its constituent school's 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)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of ours schools, DPO and DPRs and all information we are required to share about how we use and process their personal data (via our privacy notices)
    - For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

15. Data security and storage of records

We 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.

In particular:

- All staff are responsible for ensuring that any personal information, which they hold, or for which they are responsible, is kept securely. This could include information about a variety of members of the school community- including students, staff and parents/carers- e.g. legal guardianship issues, disciplinary records, progress records, reports, references, employment history, taxation and national insurance records, or appraisal records. Staff are also responsible for taking particular care when handling "sensitive personal data"- for a student this would include if they had special educational needs or if they were a "looked after child", medical information relating to them, child protection issues relating to them, their religious beliefs or political opinions, their physical or mental health issues or their sexual orientation. This would also include more logistical items such as addresses, phone numbers or dates of birth.
- Personal information stored in electronic form must be password protected.
- Computers, laptops, tablets, mobile phones and other personal devices used to store or access personal information must be locked whenever they are left unattended.
- Personal information must be kept on the network storage facilities provided.
- Personal information that is collected or processed over the internet must only be accessed via a secure encrypted connection using username authentication to prevent unauthorised disclosure.
- Personal information must not be transferred via email.

- Personal information must not be disclosed either orally or in writing or accidentally or otherwise to any unauthorised third party.
- 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
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, students, members, trustees or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment see our ICT Acceptable Use Policy.
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8)
- All staff must abide by the rules laid out in the relevant school's 'Staff ICT Acceptable Use' policy, including the 'Data Protection in the classroom' section.

See appendix 4 for further information on records retention and management.

16. Disposal of records

The MAT will comply with the requirements for the safe destruction of personal data when it is no longer required or if deletion is requested by the data subject. The disposal of data, in either paper or electronic form, must be conducted in a way that makes reconstruction highly unlikely. Electronic files must be securely overwritten, in accordance with government guidance, and other media must be shredded, incinerated, or otherwise disintegrated for data. Paper files containing sensitive information should be placed in white "confidential waste" bags/Shred It bins for shredding.

17. Personal data breaches

The MAT will make all reasonable endeavours to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 6. When appropriate, we will report the data breach to the ICO within 72 hours.

We will take actions to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach. For example: if sensitive information has been disclosed via email (including safeguarding records), we will take the following actions:

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.
- Members of staff who receive personal data sent in error must alert the sender and the DPR as soon as they become aware of the error.
- If the sender is unavailable or cannot recall the email for any reason, the DPR will ask the ICT technical support team to recall it.
- In any cases where the recall is unsuccessful, the DPR will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way.
- The DPR will ensure we receive a written response from all the individuals who received the data, confirming that they have complied with this request.
- The DPR will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted.

Other breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on one of our school's websites which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students
- A school's cashless payment provider being hacked and parents' financial details stolen

18. Training

All staff, members, trustees and governors 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 the trust's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. It will be reviewed every 2 years and shared with the Trust Board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Privacy Notices for staff, students, parents/carers, job applicants, members, trustees and governors
- Photographic Images of Children Policy
- ICT Acceptable Use Policy
- Safeguarding Policy

Appendix 1: Data protection officer (DPO)/representative (DPR)

- Ruth Allen is the DPO for the MAT and the DPR for King Charles I School. She is contactable on rallen@kingcharles1.worcs.sch.uk or at the King Charles I School on 01562 512880.
- Rob Bick is the DPR for Haybridge High School and is contactable on rcbick@haybridge.worcs.sch.uk or at school on 01562 886213.
- Jayne Sampson is the DPR for The De Montfort School and is contactable on jsampson@tdms.worcs.sch.uk or at school on 01386 442060.

Appendix 2: Information Asset Owners

- King Charles I School: The current information asset owners are as follows:

✓ SIMS and assessment data: **Simon Robinson**
✓ Exams: **Simon Robinson**
✓ Staff: **Steph Moore**
✓ ICT Support: **Stuart Wright**
✓ Safeguarding: **Chris Gibson**
✓ SEN: **Stacy Bott**
✓ Student Archives: **Chris Gibson**

- Haybridge High School: The current information asset owners are as follows:

✓ SIMS: **Tracey Davis**
✓ Assessment Data: **Rob Bick**
✓ Exams: **Julie Brown**
✓ Staff: **Gill Reynolds**
✓ ICT Support: **Paul Willetts**
✓ Safeguarding: **Nicola Stanfield**
✓ SEN: **Helen Georgiou**
✓ Student Archives: **Gill Reynolds**

- The De Montfort School: The current information asset owners are as follows:
- SIMS: **Stuart Wilson**
- Assessment Data: **Tim Dolan**
- Exams: **Sarah Reade**
- Staff: **Jayne Sampson**
- ICT Support: **Stuart Wilson**
- Safeguarding: **Fiona Lovecy**
- SEN: **Stuart Weston**
- Student Archives: **Elaine Reynolds**

Appendix 3: Parental requests to see an educational record

- King Charles I School: Please contact the school on 01562 512880 or via email at office@kingcharles1.worcs.sch.uk
- Haybridge High School: Please contact the school on 01562 886213 or via email at office@haybridge.worcs.sch.uk
- The De Montfort School: Please contact the school on 01386 442060 or via email at office@tdms.worcs.sch.uk

Appendix 4: School Records Management

The MAT recognises that by efficiently managing its records, it will be able to comply with its legal and regulatory obligations and to contribute to the effective overall management of the institution. Records provide evidence for protecting the legal rights and interests of the school, and provide evidence for demonstrating performance and accountability. This appendix provides the policy framework through which this effective management can be achieved and audited. It covers:

- Scope
- Responsibilities
- Relationships with existing policies
- Retention times

1. Scope

1.1 This appendix applies to all records created, received or maintained by staff of the school in the course of carrying out its functions.

1.2 Records are defined as all those documents which facilitate the business carried out by the school and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically.

1.3 A small percentage of the school's records might be selected for permanent preservation as part of the institution's archives and for historical research.

2. Responsibilities

2.1 The MAT has a corporate responsibility to maintain its records and record keeping systems in accordance with the regulatory environment. The person with overall responsibility for this is the CEO/executive headteacher.

2.2 The person responsible for records management in the school will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely way. They will also monitor compliance with this appendix by surveying at least annually to check if records are stored securely and can be accessed appropriately.

2.3 Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with the MAT's records management guidelines.

5. Retention Guidelines

The MAT follows the retention guidelines issued by the Management Society of Great Britain 'Retention Guidelines for Schools' (https://irms.org.uk/page/SchoolsToolkit). Some retention periods are governed by statute and others are guidelines following best practice. Every effort has been made to ensure that these retention periods are compliant with the requirements of the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000. Managing record series using these retention guidelines will be deemed to be 'normal processing' under the legislation mentioned above. If records are to be kept for longer or shorter periods than laid out in this document, the reasons for this will be documented.

Appendix 5: Subject access request form

The General Data Protection Regulation (GDPR) provides you, the data subject, with a right to receive a copy of the data/information we hold about you or to authorise someone to act on your behalf. Students who are 12 or above must make a Subject Access Request themselves.

If you wish to see your information, you can request this by contacting the relevant data protection officer (see appendix 1) or by completing the form below. You will also be required to provide proof of your identity before we can process the SAR. Your request will be processed within 30 calendar days upon receipt of a fully completed form and proof of identity.

Proof of identity

For Parents/carers who make requests on behalf of students, we require proof of your identity before we can disclose any personal information. We require you to provide two documents as proof of your identity, one should include a photograph and should include your name, date of birth and/or current address. If you have changed your name, please supply relevant documents evidencing the change. The following documents are acceptable:

- birth certificate
- passport
- driving licence
- official letter addressed to you at your address e.g. bank statement, recent utilities bill or council tax bill.

Administration fee

There is no charge for Subject Access Requests. However, there may be a charge for providing duplicate information and/or dealing with excessive requests. The will be based upon the amount of time spent dealing with the request.

Section 1

Is the person who the Subject Access Request is about a: **Student** or an **Employee** (please delete which ever does not apply)
If the person who the Subject Access Request is about is no longer a student or employed by King Charles I School, Haybridge High School or The De Montfort School School: ……. Date Started …… Date left ……

Please fill in the details of the data subject in part A. Only complete part B, if you are not the data subject and are applying on behalf of someone else.

Part A Details of the persons who the subject access request is about.	**Part B** Details of the person making the request on behalf of a student under 13 years of age
Title: Mr ☐ Mrs ☐ Ms ☐ Miss ☐ Other ☐	Title: Mr ☐ Mrs ☐ Ms ☐ Miss ☐ Other ☐
Surname / Family Name:	Surname / Family Name:
Is there any other Surname / Family Name name that may have been used at school	
First names(s) / Forenames:	First names(s) / Forenames:
Date of Birth	Date of Birth
Address: Post Code:	Address: Post Code:
Day Time Telephone Number (s)	Day Time Telephone Number (s)

Appendix 6: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the relevant DPR. The relevant DPR will alert the DPO and take advice regarding the investigation.
- The relevant DPR will investigate the report and determine whether a breach has occurred. To decide, they will consider whether personal data has been accidentally or unlawfully:
  - Lost
  - Stolen
  - Destroyed
  - Altered
  - Disclosed or made available where it should not have been
  - Made available to unauthorised people

The DPR will discuss the outcome of the investigation with the DPO.

- The DPO will alert the relevant associate headteacher, the chair of the relevant local governing body and the CEO/executive headteacher. The CEO/executive headteacher will contact the chair of the Trust Board.
- The DPR will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. For example:
- The DPR will assess the potential consequences, based on how serious they are, and how likely they are to happen and write a report and present it to the DPO.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 72 hours. As required, the DPO will set out:
  - A description of the nature of the personal data breach including, where possible:
    - ✓ The categories and approximate number of individuals concerned
    - ✓ The categories and approximate number of personal data records concerned
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
- If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:
  - The name and contact details of the DPO
  - A description of the likely consequences of the personal data breach
  - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
- The DPO will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
- The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
  - Facts and cause
  - Effects
  - Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)

  Records of all breaches will be stored securely on the school computer system.
- The DPO, relevant associate headteacher and DPR will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.