Data Protection Policy

Healing Multi Academy Trust

Author and Reviewer	Lindsey Smith – DPO
Date adopted by Healing Multi - Academy Trust	May 2018
Reviewed	May 2020
Consultations / Training	All Staff
Linked Policies	Acceptable Use Policy Freedom of information publication scheme Child Protection/Safeguarding Policy Retention of Records Management Policy

Contents

1. Aims

Healing Multi Academy trust (Trust) aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected 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.

Schools within the Trust must meet the requirements of the Protection of Freedoms Act 2012 when referring to the use of biometric data.

This policy 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.

This policy also complies with the Trust's 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

Schools within Healing MAT process personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

The Trust 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 Healing MAT, and to external organisations or individuals working on our behalf. Failure to comply with this policy may lead to disciplinary action.

5.1 Healing Multi – Academy Trust board

The MAT Board of Trustees has overall responsibility for ensuring all Trust schools comply with all relevant data protection obligations.

5.2 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 will provide a regular termly report of activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on education data protection issues.

The DPO is also the first point of contact for individuals whose data the schools process, and for the ICO.

Full details of the DPO's responsibilities are set out in their job description.

The Trust's DPO is contactable via DPO@healingmultiacademytrust.co.uk or via telephone on 01472 582525

5.3 Headteacher & CEO

The Headteacher of the school is responsible as the data controller on a day-to-day basis. The CEO has overall accountability as the data controller for the Trust.

5.4 All staff

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Informing the Headteacher (Data Controller) with regards to:
  - any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - any concerns that this policy is not being followed
  - being unsure whether or not they have a lawful basis to use personal data in a particular way
  - capturing consent, drafting a privacy notice, dealing with data protection rights invoked by an individual, or transferring personal data outside the European Economic Area
  - reporting a data breach
  - engaging in a new activity that may affect the privacy rights of individuals
  - help with any contracts or sharing personal data with third parties

6. Data protection principles

The GDPR is based on data protection principles that must be complied with.

The principles state 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 Trust will 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 school 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 school 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 schools, 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 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 pupil) has freely given clear **consent**

For special categories of personal data, one of the special category conditions must be met for processing, which are set out in the GDPR and Data Protection Act 2018.

If Trust schools offer online services to pupils, such as classroom apps, and rely on consent as a basis for processing, parental consent must be obtained if the pupil is aged 12 and under (except for online counselling and preventive services).

Whenever personal data is initially collected directly from individuals, relevant information required by data protection law will be provided to them.

7.2 Limitation, minimisation and accuracy

Personal data must only be collected for specified, explicit and legitimate reasons. These reasons must be explained to the individuals when their data is first collected.

If personal data is to be used for reasons other than those given initially, individuals concerned must be informed and consent sought where necessary.

Staff must only process personal data where it is necessary in order to do their jobs.

When personal data held is no longer required, it must be deleted or anonymised. This must be done in accordance with the Trust Retention of Records Management Policy.

8. Sharing personal data

Personal data must not be shared with anyone else, and can only be considered if:

- There is an issue with a pupil or parent/carer that puts the safety of staff at risk
- There is a need to liaise with other agencies – consent may be required prior to doing this
- Suppliers or contractors need data to enable services to be provided to staff and pupils – for example, IT companies. The Trust must:
    - Only appoint suppliers or contractors which can provide sufficient guarantees of compliance 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 shared
    - Only share data that the supplier or contractor needs to carry out their service

Personal data can be shared with law enforcement and government bodies where there are legal requirements to do so, including:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- Information connection with legal proceedings

- Disclosing information required to satisfy safeguarding obligations
- Research and statistical purposes, as long as personal data is anonymised or consent has been provided

Personal data may also be shared with emergency services and local authorities to help them to respond to an emergency situation that affects any pupil or staff member.

If personal data is transferred to a country or territory outside the European Economic Area, it must be done 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 Trust or schools hold about them. This may include:

- 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

Subject access requests must be submitted in writing, either by letter or email to the School's Headteacher. They should include:

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

The Trust's DPO must be informed as soon as any subject access request is received. The DPO will log all Subject Access Requests be logged onto the Trust's GDPR software.

9.2 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.

Children aged 12 and under 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 pupils in primary schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 13 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 pupils at secondary school may not be granted without the express written permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests

In all cases the DPO must be informed.

When responding to requests:

- Ask the individual to provide identification
- Contact the individual via phone to confirm the request was made
- Respond without delay and within 1 month of receipt of the request
- Provide the information free of charge
- Tell the individual, compliance will be within 3 months of receipt of the request, where a request is complex (the meaning of 'complexity' as used in the SAR provisions of the GDPR would likely be fact and context dependent. The GDPR suggests that where the employer processes a large quantity of information about the employee/ pupil it should ask them to "specify the information or processing activities to which the request relates".) or numerous. The individual must be informed of this within 1 month, with an explanation why the extension is necessary

Information may not be disclosed if it:

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

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 unfounded if the individual has no clear intention to access the information or is malicious in intent and is using the request to harass an organisation with no real purposes other than to cause disruption. The request will be deemed excessive if it is repetitive, asks for further copies of the same information or overlaps with other requests.

When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

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 the school 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 DPO. If staff receive such a request, they must immediately forward it to the DPO.

10. Biometric recognition systems

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

Parents/carers must be notified before any biometric recognition system is put in place or before their child first takes part in it. The school must obtain 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 pupils have the right to choose not to use the school's biometric system(s). Alternative means of accessing the relevant services for those pupils must be provided in such cases.

Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time and any relevant data already captured must be deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, this data cannot be processed, irrespective of any consent given by the pupil's parent(s)/carer(s).

Where staff members or other adults use the school's biometric system(s), their consent must be obtained 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 must delete any relevant data already captured.

11. CCTV

CCTV is used in various locations around MAT school sites to ensure they remain safe environments. The ICO's code of practice for the use of CCTV must be adhered to.

Individuals' permission to use CCTV is not required, but it must be clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. The CCTV footage is only used for the intended purpose. It may be shared with the Police if required and can be viewed by any person appearing on the footage via the Subject Access Request criteria.

Any enquiries about the CCTV system in each school should be directed to the Headteacher.

12. Photographs and videos

As part of our school activities, photographs and record images of individuals may be taken within schools.

Written consent must be obtained from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. It must be clearly explained to both the parent/carer and pupil how the photograph and/or video will be used.

This may 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 school or MAT websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the photograph or video will be deleted and not distributed further.

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

13. Data protection by design and default

General Data Protection Regulation measures must be in place to integrate 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 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
- Providing training for 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 privacy measures and ensure compliance
- Maintaining records of processing activities, including:
    - For the benefit of data subjects, making available the name and contact details for schools and the DPO and all information we are required to share about how personal data is used and processed (via our privacy notices)
    - For all personal data held, maintaining an internal record of the type of data, data subject, how and why the data is used, any third-party recipients, how and why data is stored, retention periods and how the data is kept secure

14. Data security and storage of records

Personal data will be protected and kept it safe from unauthorised or unlawful access, alteration, process or disclosure, and against accidental or unlawful loss, destruction or damage.

In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- 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
- Where personal information needs to be taken off site, staff must ensure electronic data is encrypted and paper-based data is kept in a safe location and returned to school for correct disposal
- Passwords used to access school computers, laptops and other electronic devices should be at least 8 characters long and contain upper and lower case letters and numbers. Staff and pupils 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, pupils 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 *acceptable use policy*)
- Where personal data has to be shared with a third party, due diligence is carried out and reasonable steps taken to ensure it is stored securely and adequately protected (see section 8)

15. Disposal of records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where it cannot or does not need to be rectified or updated.

Paper-based records will be shredded or incinerated, and electronic files will be overwritten or deleted. A third party may be used to safely dispose of records on the Trust's behalf. Any third party must provide sufficient guarantees that they comply with data protection law.

16. Personal data breaches

The Trust and all schools must make reasonable endeavours to ensure that there are no personal data breaches.

In the unlikely event of a suspected data breach, the procedures set out in appendix 1 must be followed.

When appropriate, the data breach must be reported to the ICO within 72 hours. Such breaches in a school context may include, but are not limited to:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils 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 pupils
- Data about one pupil being sent home to another parent

17. Training

All staff and governors will be provided with data protection training as part of their induction process.

Data protection will also form part of continuing professional development. Changes to legislation, guidance or any Trust school's processes will form part of this.

18. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed annually and shared with the LGBs and the MAT Board.

Appendix 1: 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 Headteacher, DPO and CEO
- The Headteacher & DPO 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 Headteacher, DPO and CEO will inform the Chair of Governors and the Chair of the MAT Board
- The Headteacher, DPO and CEO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out at the end of this procedure)
- The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
- The DPO (together with the CEO) will determine 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. Documented decisions are stored using the Trust's GDPR recording and reporting software.
- 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 using the Trust's GDPR recording and reporting software. The DPO, CEO and Headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

The actions set out below will be taken to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. The effectiveness of these actions will be reviewed and amended as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- 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 Headteacher as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the Headteacher will ask for ICT support to recall it
- In any cases where the recall is unsuccessful, the Headteacher 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 DPO will ensure a written response is received from all the individuals who received the data, confirming that they have complied with this request

- The DPO will carry out an internet search to check that the information has not been made public; if it has, the publisher/website owner or administrator will be contacted to request that the information is removed from their website and deleted

Other types of breach and processes may include:

- If details of any pupil premium interventions for named children are published on a school website, this must be removed as soon as possible and reported to the Headteacher. The SENDCo or Headteacher must then inform the parents of the situation and that the information has been subsequently removed.
- All pupil exam results or staff pay information shared with governors or trustees must be anonymised. If any personal data is made available, it must be immediately withdrawn and not recorded in the minutes of the meeting. The DPO and Headteacher must be informed and arrangements will be made to inform the member of staff.
- If any item of school equipment including a laptop, tablet or mobile telephone is lost, stolen or hacked, the Headteacher must be informed immediately. All equipment and data should be password protected. If any staff member, governor or trustee becomes aware a school laptop containing non-encrypted sensitive personal data being stolen or hacked, they must inform the Headteacher and DPO as soon as possible. The loss must be reported to the police and the DPO will take action to inform the ICO within the required timescales.
- If any third party contacts the Trust to report a data breach and sensitive data has been stolen e.g. the school's cashless payment provider being hacked and parents' financial details stolen, then the DPO must be informed immediately. The DPO will acquire all information available and make arrangements to inform the ICO and make telephone and written contact with all affected parents as soon as possible.