Washwood Heath
Multi Academy Trust

GDPR Data Protection Policy

Prepared by:	Director of HR in consultation with GDPR Working Group
Applies to:	Employees at WHMAT Academies (right to make subject access requests extend to all relevant individuals)
Approved by:	WHMAT Board of Trustees following consultation with GDPR working group, whole school staff and Data Protection Officer (DPO)
Issued to WHMAT Academies for use:	22.05.2018
Annual review date:	24 months from ratification by Board of Trustees
Links to:	WHMAT's GDPR Compliant Data Retention Policy WHMAT's Freedom of Information Policy WHMAT's E-Safety Policy WHMAT's Disciplinary Policy & Procedure ICO's Code of Practice for use of CCTV WHMAT's Safeguarding & Child Protection Policy WHMAT's Employee Code of Conduct WHMAT's GDPR Managers' Toolkit
Version:	Version 4. 22.05.18

Contents

1. Aims

1.1 Washwood Heath Multi Academy Trust (WHMAT) aims to ensure that all personal data collected about staff, pupils, parents, governors, trustees, visitors and other individuals is collected, stored and processed in accordance with the *General Data Protection Regulation (GDPR)* and the *Data Protection Act 2018 (DPA 2018).*

1.2 WHMAT is committed to being transparent about how it collects and uses the personal data of its workforce, pupils and stakeholders and to meeting its data protection principles.

1.3 This policy sets out WHMAT's commitment to data protection, and individual rights and obligations in relation to personal data. It applies to all personal data, regardless of whether it is in paper or electronic format.

1.4 Any references in this policy to WHMAT, also refer to individual academies within WHMAT.

2. Legislation and guidance

2.1 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.*

2.2 It meets the requirements of the *Protection of Freedoms Act 2012* when referring to WHMAT's use of biometric data.

2.3 It also reflects the *ICO's code of practice for the use of surveillance cameras and personal information.*

3. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual, who can be identified from that information. That living individual may be an employee, contractor, parent, pupil, trustee, volunteer or supplier

	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 "sensitive 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 living individual whose personal data is held or processed e.g. a member of staff, pupil, trustee, parent etc.
Data controller	A person or organisation that determines the purposes and the means of processing personal data e.g. WHMAT

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 e.g. an outsourced payroll provider or contractor
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data
Criminal records data	Information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings

4. The data controller

4.1 WHMAT processes personal data relating to parents, pupils, staff, governors, trustees, visitors and others, and therefore is a "data controller".

4.2 WHMAT is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. Roles and responsibilities

5.1 This policy applies to all staff employed by WHMAT, and to external organisations or individuals working on our behalf. All staff must read this Policy carefully and make sure that they are familiar with it. Staff who do not comply with this policy may face disciplinary action in line with *WHMAT's Disciplinary Policy & Procedure*.

5.2 Staff who believe that fellow colleagues are not complying with data protection laws and/or this Policy are encouraged to report this to the DPO at dpo@washwoodconnect.com or via our confidential WHMAT Whistleblowing Policy.

WHMAT's Board of trustees

5.3 WHMAT's Board of trustees has overall responsibility for ensuring that WHMAT academies comply with all relevant data protection obligations.

Data Protection Officer (DPO)

5.4 The 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.

5.5 The DPO will provide an annual report of their activities directly to WHMAT's board of trustees and, where relevant, report to the board their advice and recommendations on data protection issues. The DPO is also the first point of contact for individuals whose data WHMAT processes, and for the ICO. Our DPO is James Plant of Services for Schools and is contactable at dpo@washwoodconnect.com.

5.6 If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with your base academy data protection lead in the first instance (see www.washwoodmat.com policies section for list of contacts). Alternatively, you can contact the Information Commissioner's Office direct at https://ico.org.uk/concerns/

Heads of Academy

5.7 Individual Heads of Academy act as representatives of the data controller, WHMAT, on a day-to-day basis and must do all that they reasonably can to ensure that data is processed in accordance with the key data protection principles set out in law (see further at 6 below).

HR

5.8 HR colleagues are responsible for ensuring that personal data gathered during the employment, worker, contractor, volunteer or apprenticeship relationship is held in the individual's HR/personnel file (in hard copy or electronic format, or both), and on HR systems. The periods for which WHMAT holds HR-related personal data are contained in its privacy notices to individuals and in *WHMAT's GDPR Data Retention Policy.*

All staff

5.9 Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Promptly informing their base academy HR contact of any changes to their personal data, such as a change of address or contact number
- Contacting the DPO and ensuring that the base academy data protection lead is copied into any correspondence, 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

The Information Commissioner (ICO)

5.10 The ICO is the regulator for data protection in the UK. It has extensive powers, including the ability to impose civil fines (currently of up to 20 million Euros or 4% of turnover, whichever is higher.

6. Data protection principles

6.1 The GDPR is based on data protection principles that WHMAT 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

6.2 This policy sets out how WHMAT aims to comply with these principles.

7. Collecting personal data

Lawfulness, fairness and transparency

7.1 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 WHMAT can **fulfil a contract** with the individual, or the individual has asked WHMAT to take specific steps before entering into a contract
- The data needs to be processed so that WHMAT 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 WHMAT, 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 WHMAT 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**

7.2 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.*

7.3 If WHMAT primary academies offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent (except for online counselling and preventive services).

7.4 If WHMAT secondary academies offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will obtain parental consent where the pupil is under 13.

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

Limitation, minimisation and accuracy

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

7.7 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.

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

7.9 When staff no longer need the personal data they hold, they must ensure it is deleted, anonymized or destroyed in accordance with *WHMAT's GDPR Compliant Data Retention Policy.*

8. Sharing personal data

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

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk (see also WHMAT's Safeguarding & Child Protection Policy)
- We need to liaise with other external agencies – we will seek consent as necessary before doing this (subject to any limitations imposed by safeguarding matters)
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – 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

8.2 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

8.3 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 pupils or staff.

8.4 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

Subject access requests

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

- Confirmation that their personal data is being processed
- Access to a copy of the data
- The reasons why their data is being processed/purposes
- 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

9.2 Subject access requests must be submitted in writing to the DPO at dpo@washwoodconnect.com, either by letter, email or via WHMAT's online form located at www.washwoodmat.com. It should be copied to the base academy data protection lead (see details under policies tab www.washwoodmat.com). The request should include:

- Name of individual making the request
- Correspondence address
- Contact number and email address, where one exists
- Details of the information requested

9.3 If WHMAT staff receive a subject access request they must immediately forward it to the DPO at dpo@washwoodconnect.com.

Children and subject access requests

9.4 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.

9.5 Children below the age of 12 i.e. in our WHMAT primary academies, 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 WHMAT pupils may be granted without the express permission of the pupil. However, this is not a rule and a pupil's ability to understand their rights will always need to be judged on a case-by-case basis by the Head of Academy or other appropriate manager, in consultation with the DPO.

9.6 Children aged 12 and above i.e. in our WHMAT secondary academies 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 WHMAT pupils may not be granted without the express permission of the pupil. Again, this is not a rule, and a pupil's ability to understand their rights will always need to be judged on a case-by-case basis by the Head of Academy or other appropriate manager, in consultation with the DPO.

Responding to subject access requests

9.7 When responding to requests, we:

- May ask the individual to provide 2 forms of identification before the request can be processed
- May contact the individual via phone to confirm the request was made
- Will normally respond without delay and within 1 month of receipt of the request. If, however, WHMAT processes large amounts of the individual's data, or the request is complex or numerous, it may respond within 3 months of the date the request is received. In these circumstances, WHMAT will write to the individual within one month of receiving the original request to explain to him or her if this is the case and the reasons why
- Will provide the information free of charge

9.8 We will not disclose information 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
- Would otherwise lead to a breach of *WHMAT's Safeguarding & Child Protection Policy & Procedure*

Advice shall be sought from the DPO before refusing to disclose information that is requested by an individual in these circumstances.

9.9 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.

9.10 A request will be deemed to be unfounded or excessive if it is repetitive, or asks for further copies of the same information.

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

10. Other data protection rights of the individual

10.1 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 a number of other rights in relation to their personal data. For example, they can ask WHMAT to:

- Rectify inaccurate data;
- Stop processing or erase data that is no longer necessary for the purposes of processing;
- Stop processing or erase data if the individual's interests override WHMAT's legitimate grounds for processing data (where WHMAT relies on its legitimate interests as a reason for processing data);
- Stop processing or erase data if processing is unlawful;
- Prevent use of their personal data for direct marketing;
- Stop processing or erase data which has been justified on the basis of public interest grounds;
- Provide a copy of agreements under which their personal data is transferred outside of the European Economic Area;
- Refrain from taking 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, unless this is being done in good faith in line with *WHMAT's Safeguarding & Child Protection Policy*;
- 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.

10.2 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 at

dpo@washwoodconnect.com or by post to S4S, Midlands Technology Centre, Broadlands, Wolverhampton, WV10 6TA.

11. Parental requests to see the educational record

11.1 WHMAT offers discretionary access to parents, or those with parental responsibility, to free access to their child's educational record (which includes most information about a pupil) within a reasonable period of a written request.

12. Biometric recognition systems

12.1 Where we 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), we will comply with the requirements of the *Protection of Freedoms Act 2012* (note that under this legislation, a "child" means a person under the age of 18).

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

12.3 Parents/carers and pupils have the right to choose not to use WHMAT's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

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

12.5 As required by law, if a pupil 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 pupil's parent(s)/carer(s).

12.6 Where staff members or other adults use WHMAT'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 WHMAT will delete any relevant data already captured.

13. CCTV

13.1 WHMAT understands that recording images of identifiable individuals is classed as "processing personal information", so must comply with data processing principles under this policy.

13.2 Across WHMAT, we use CCTV in various locations to ensure it remains secure. WHMAT will adhere to the *ICO's code of practice for the use of CCTV*. We will notify all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

13.3 We do not need to ask individuals' permission to use CCTV, but we will make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

13.4 We will ensure that cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

13.5 All CCTV footage will be kept for 28 calendar days for security purposes, before being deleted, unless subject to a criminal or internal investigation.

13.6 Any enquiries about CCTV systems across WHMAT sites should be directed to Mr Delroy Bramwell (Director of Estates for WHMAT) on 0121 675 7272 or Washwood Heath Multi Academy Trust, Burney Lane, Stechford, B1 2AS.

14. Photographs and videos

14.1 As part of our day-to-day academy activities, we may take photographs and record images of individuals within WHMAT.

14.2 In WHMAT primary academies, we will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

14.3 In WHMAT secondary academies, we will obtain written consent from parents/carers, or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing and promotional materials.

14.4 Where we need parental consent to use images/video footage, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

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

14.6 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 *WHMAT's Safeguarding and Child Protection Policy* for more information on our use of photographs and videos. Heads of Academy and other appropriate managers are reminded to warn parents and carers not to post school photos or performances containing pupils, other than their own, on social media channels.

15. Data protection by design

15.1 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 data protection impact assessments (DPIAs) where WHMAT'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 – see further below at 20)
- 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; ensuring we 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 our DPO 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 (known as a data audit).

16. Data security and storage of records

16.1 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.

16.2 In particular, all staff will ensure that:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are stored securely and kept under lock and key when not in use;
- Documents and databases containing personal data are password protected;
- Papers containing confidential personal data are not left unattended on office and/or classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
- When viewing personal data on computer screens, specialist screen covers are used or that this is not viewed by others;
- Confidential paper records are kept in a locked filing cabinet, drawer or safe, with restricted access;
- Emails do not contain sensitive or confidential information, in either the title or main text of the email but are, instead, sent via a password-protected attachment;
- Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients;
- Before sharing data, a) they are allowed to share it, b) adequate security is in place to protect it; and c) that who will receive the data has been outlined in a privacy notice;
- Personal data about staff and/or pupils is not on display in offices, classrooms or other accessible areas within WHMAT premises;
- Items containing personal data (paper files, mobile phones, laptops, tablets, memory sticks etc.) are not left unattended in a public place, e.g. on a train, in a café etc. or in unsecure places, such as in a car overnight;
- Where personal information needs to be taken off site, for example staff or pupil data, that it is stored safely and securely;
- Passwords that are at least 6 characters long containing letters and numbers are used to access WHMAT computers, laptops and other electronic devices;
- Staff and pupils are actively reminded to change their passwords at regular intervals;
- Encryption software is used to protect all staff laptops;
- All USB and/or alternative storage devices being used to hold sensitive information must be encrypted by IT before usage;
- Staff, pupils, governors or trustees who store personal information on their personal devices are expected to follow the same security procedures as for academy-owned equipment, ensuring password protection as a minimum (see our E-Safety 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.

17. Disposal of records

17.1 Personal data that is no longer needed will be disposed of securely in line with *WHMAT's GDPR Compliant Data Retention Policy*.

17.2 Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it. For example, we will shred paper-based records and overwrite or delete electronic files.

17.3 We may also use a third party to safely dispose of records on WHMAT's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

18. Personal data breaches

18.1 WHMAT will make all reasonable endeavours to ensure that there are no personal data breaches.

18.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in appendix 1.

18.3 When appropriate, the DPO will report the data breach to the ICO within 72 hours. Such breaches in an academy context may include, **but are not limited to**:

- A non-anonymised dataset being published on the WHMAT website or shared via email, which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of or loss of a WHMAT laptop or memory stick containing non-encrypted personal data about pupils and/or staff
- Details of pupil premium interventions for named children being published on base academy or WHMAT website
- Non-anonymised pupil exam results or staff pay information being shared with governors, trustees or advisory boards
- An academy laptop containing non-encrypted sensitive personal data being stolen, lost or hacked
- The cashless payment provider in a WHMAT academy being hacked and parents' financial details stolen.

(see further at appendix 1)

19. Training

19.1 All WHMAT staff will be required to complete online GDPR training. In addition, staff will be required to complete refresher training at regular intervals.

19.2 Heads of Academy (Deputy CEO for Head Office staff) will ensure that staff receive training on this Policy once it has been ratified by the Board of Trustees.

19.3 WHMAT Advisory Boards and trustees will be provided with GDPR training.

19.4 Data protection will also form part of continuing professional development, where changes to legislation, guidance or WHMAT's processes make it necessary.

20. Data Protection Impact Assessments (DPIAs)

20.1 DPIAs will be used to identify the most effective method of complying with WHMAT's data protection obligations and meeting individuals' expectations of privacy. They will allow WHMAT to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to WHMAT's reputation which might otherwise occur.

20.2 A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

20.3 A DPIA will be used for more than one project, where necessary. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences
- The use of CCTV
- Changing the way school dinners are paid for e.g. introduction of biometric recognition systems
- Changing the way staff are required to keep pupil behaviour records.

20.4 WHMAT will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals

- The measures implemented in order to address risk

20.5 Where a DPIA indicates high risk data processing, the relevant base academy data protection contact will consult the DPO for advice on GDPR compliance.

21. Policy Review

21.1 The GDPR Working Group is responsible for monitoring and reviewing this policy.

21.2 It will be reviewed and updated every 24 months from ratification by the board of trustees, unless changes to associated legislation or good practice require an earlier review.

22. Links with other policies

22.1 This policy is linked to a number of other internal and external policies, guidance and documents as set out on the front page.

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 DPO at dpo@washwoodconnect.com. The relevant base academy data protection contact should also be copied into this email unless the disclosure is potentially a confidential whistleblowing matter;
- The DPO will investigate the alleged data breach, and determine whether a breach has occurred.
- To decide whether a breach has occurred, the DPO 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 DPO will alert the relevant head of academy and/or the chair of trustees, where deemed appropriate
- The DPO 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 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 will be stored in a risk register.
- 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 on each base academy's data audit spreadsheet.
- The DPO and relevant head of academy (Deputy CEO for breaches relating to head office staff or data), will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible. In these circumstances, the head of academy will be responsible for sharing this information to the CEO, Deputy CEO and other WHMAT heads, so that lessons can be learnt and appropriate interventions or training put in place.

Actions to minimise the impact of data breaches

We will take the actions set out below 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.

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 DPO as soon as they become aware of the error
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask IT support to recall it
- In any cases where the recall is unsuccessful, the DPO 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 we receive a written response 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, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted