Christ Centred, Child Centred, Catholic Educational Excellence

THE DIOCESE OF WESTMINSTER ACADEMY TRUST

DATA PROTECTION AND BREACH RESPONSE POLICY

This Data Protection and Breach Response Policy has been approved and adopted by The Diocese of Westminster Academy Trust in May 2025 and will be reviewed in May 2027.

Signed by the Chair of The Diocese of Westminster Academy Trust:

CONTENTS

1. INTRODUCTION

1.1 The objectives of this Data Protection Policy are to ensure that the Diocese of Westminster Academy Trust (the "Trust") and its directors, local governors, members and employees are informed about, and comply with, their obligations under the UK General Data Protection Regulation ("the UK GDPR") and other data protection legislation.

1.2 This is an internal policy which works alongside data protection logs, procedures and Privacy Notices. It is to be read in conjunction with the school Privacy Notice (website) and Privacy Notice for Staff, Governors and Volunteers (internal policy).

1.3 Where 'school' is stated within this policy, this could be actioned by the Trust, on behalf of a member school. Where DPO (Data Protection Officer) is stated, this could be actioned by either the Trust External or Internal DPO or the school Deputy DPO also known as the School Data Protection Lead.

1.4 The Trust is a Multi Academy Trust and is the Data Controller for all the Personal Data processed by its academies and by the central team at the Trust. For a list of the academies within the Trust, please follow this link: https://www.dowat.co.uk/12/our-schools

1.5 The procedures set out in this document are particularly important as, prior to the UK GDPR, there was no obligation on the school to notify the Information Commissioner's Office ('ICO') of data security breaches, although it was good practice to report serious breaches.

1.6 In addition to detailing Data Protection organisation within the Trust and its Schools, this document also sets out how we will respond to any suspected or actual data breaches and should be read alongside school GDPR procedural documentation.

1.7 The UK GDPR requires each school, or the Trust on behalf of one of its member schools, to report 'notifiable breaches' without undue delay and, where feasible, not later than 72 hours after having become aware of it. Notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, which is a subjective measure determined jointly by the Data Breach Response Team. In the event that a report is not made within 72 hours, the school is required to provide the reasons for the delay in reporting it to the ICO.

1.8 If there is deemed to be a "high risk" to the rights and freedoms of individuals following a data breach, the school is also required to notify the individuals affected by the breach. However, in the interests of transparency, the school recognise that on some occasions it will be appropriate to notify affected individuals, even if we are not legally obliged to do so.

1.9 If the School fails to report a notifiable personal data breach, we are at risk of receiving a sanction from the ICO, which may include a fine. Aside from our desire to avoid receiving any sanctions, the purpose of this policy is to ensure that we protect the Personal Data of our stakeholders and minimise any risks to them following a breach.

1.10 The School will ensure that staff are aware of and are trained on UK GDPR and data security at least biennially.

1.11 We rely on our staff to be alert to the risk of data security breaches and to follow the procedures set out in this policy to ensure that we can react promptly in the event that a breach or suspected breach occurs. Any member of staff who becomes aware of a suspected or actual personal data breach must follow the escalation procedures set out below. Failure to comply with these procedures may be a disciplinary issue.

1.12 This policy does not form part of any employee's contract of employment and it may be amended at any time. Any breach of this policy by members of staff will be taken seriously and may result in disciplinary action and serious breaches may result in dismissal. Breach of the UK GDPR may expose the Trust to enforcement action by the Information Commissioner's Office (ICO) or fines. Furthermore, certain breaches of the Act can give rise to personal criminal liability for the Trust's employees. At the very least, a breach of the UK GDPR could damage our reputation and have serious consequences for the Trust and for our stakeholders.

2. DATA PROTECTION OFFICER

2.1 The Data Protection Officer (the "DPO") is responsible for ensuring the Trust is compliant with the UK GDPR and with this policy. This post is held at Trust level by the Chief Financial Officer, supported by an External DPO Richard Maskrey. The Trust DPO can be contacted via the 'Contact Us' form on the Trust website https://www.dowat.co.uk/148/contact-us-1 or via email at dpo@dowat.co.uk. In addition, an internal Deputy DPO will be appointed at each academy within the Trust and will report to the Trust DPO on matters relating to data protection compliance, to be known as the Academy Data Protection Lead. Any questions or concerns about the operation of this policy should be referred in the first instance to the Internal Trust DPO.

2.2 The DPO will play a major role in embedding essential aspects of the UK GDPR into the Trust's culture, from ensuring the data protection principles are respected to preserving data subject rights, recording data processing activities and ensuring the security of processing.

2.3 The DPO should be involved, in a timely manner, in all issues relating to the protection of personal data. To do this, the UK GDPR requires that DPOs are provided with the necessary support and resources to enable the DPO to effectively carry out their tasks. Factors that should be considered include the following:

2.3.1 Senior management support;

2.3.2 Time for Deputy DPOs to fulfil their duties;

2.3.3 Adequate financial resources, infrastructure (premises, facilities and equipment) and staff where appropriate;

2.3.4 official communication of the designation of the DPO to make known existence and function within the organisation;

2.3.5 access to other services, such as HR, IT and security, who should provide support to the Trust DPO;

2.3.6 continuous training so that Deputy DPOs can stay up to date with regard to data protection developments;

2.3.7 where a DPO team is deemed necessary, a clear infrastructure detailing roles and responsibilities of each team member;

2.3.8 whether the Trust should give the DPO access to external legal advice to advise the DPO on their responsibilities under this Data Protection Policy.

2.4 The DPO is responsible for ensuring that the Trust's Processing operations adequately safeguard Personal Data, in line with legal requirements. This means that the governance structure within the Trust must ensure the independence of the DPO.

2.5 The Trust will ensure that the DPO does not receive instructions in respect of the carrying out of their tasks, which means that the DPO must not be instructed how to deal with a matter, such as how to investigate a complaint or what result should be achieved. Further, the DPO should report directly to the highest management level, i.e. the board of directors.

2.6 The requirement that the DPO reports directly to the board of directors ensures that the Trust's directors are made aware of the pertinent data protection issues. In the event that the Trust decides to take a certain course of action despite the DPO's advice to the contrary, the DPO should be given the opportunity to make their dissenting opinion clear to the board of directors and to any other decision makers.

3. DEFINITION OF TERMS

3.1 Biometric Data means Personal Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images;

3.2 Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to them;

3.3 Data is information which is stored electronically, on a computer, or in certain paper-based filing

systems or other media such as CCTV;

3.4 Data Subjects for the purpose of this policy include all living individuals about whom we hold Personal Data. A Data Subject need not be a UK national or resident. All Data Subjects have legal rights in relation to their Personal Data.

3.5 Data Controllers means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data.

3.6 Data Users include employees, volunteers, trustees [and local governors] whose work involves using Personal Data. Data Users have a duty to protect the information they handle by following our data protection and security policies at all times;

3.7 Data Processors means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller;

3.8 Parent has the meaning given in the Education Act 1996 and includes any person having parental responsibility or care of a child;

3.9 Personal Data means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

3.10 Personal Data Breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

3.11 Privacy by Design means implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the UK GDPR;

3.12 Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3.13 Sensitive Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

4. DATA PROTECTION PRINCIPLES

4.1 Anyone processing Personal Data must comply with the enforceable principles of good practice. These provide that Personal Data must be:

4.1.1 processed lawfully, fairly and in a transparent manner in relation to individuals;

4.1.2 collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

4.1.3 adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

4.1.4 accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

4.1.5 kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed; Personal Data may be stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals; and

4.1.6 Processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. PROCESSED LAWFULLY, FAIRLY AND IN A TRANSPARENT MANNER

5.1 The UK GDPR is intended not to prevent the processing of Personal Data, but to ensure that it is done fairly and without adversely affecting the rights of the Data Subject. The Data Subject must be told who the Data Controller is (in this case the Trust), who the Data Controller's representative is (in this case the DPO), the purpose for which the data is to be Processed by us, and the identities of anyone to whom the Data may be disclosed or transferred.

5.2 For Personal Data to be processed lawfully, certain conditions have to be met. These may include:

5.2.1 where we have the Consent of the Data Subject;

5.2.2 where it is necessary for compliance with a legal obligation;

5.2.3 where processing is necessary to protect the vital interests of the Data Subject or another person;

5.2.4 where it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

5.3 Personal data may only be processed for the specific purposes notified to the Data Subject when the data was first collected, or for any other purposes specifically permitted by the Act. This means that Personal Data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the Data Subject must be informed of the new purpose before any processing occurs.

5.4 The Trust will be processing Sensitive Personal Data about our stakeholders. We recognise that the law states that this type of Data needs more protection. Therefore, Data Users must be more careful with the way in which we process Sensitive Personal Data.

5.5 When Sensitive Personal Data is being processed, as well as establishing a lawful basis (as outlined in paragraph 5.3 above), a separate condition for processing it must be met. In most cases the relevant conditions are likely to be that:

5.5.1 the Data Subject's explicit consent to the processing of such data has been obtained

5.5.2 processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, where we respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;

5.5.3 processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;

5.5.4 processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Data Controller or of the Data Subject in the field of employment law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject.

5.6 The Trust recognises that in addition to Sensitive Personal Data, we are also likely to Process information about our stakeholders which is confidential in nature, for example, information about family circumstances, child protection or safeguarding issues. Appropriate safeguards must be implemented for such information, even if it does not meet the legal definition of Sensitive Personal Data.

5.7 Academies in the Trust may process Biometric Data as part of an automated biometric recognition

system, for example, for cashless catering or photo ID card systems where a pupil's photo is scanned automatically to provide them with services. Biometric Data is a type of Sensitive Personal Data.

5.8 Where Biometric Data relating to pupils is processed, the relevant academy must ensure that each parent of a child is notified of the school's intention to use the child's Biometric Data and obtain the written consent of at least one parent before the data is taken from the pupil and used as part of an automated biometric recognition system. An academy must not process the Biometric Data of a pupil under 18 years of age where:

5.8.1 the child (whether verbally or non-verbally) objects or refuses to participate in the Processing of their Biometric Data;

5.8.2 no Parent has Consented in writing to the processing; or

5.8.3 a Parent has objected in writing to such processing, even if another Parent has given written Consent.

5.9 Academies must provide reasonable alternative means of accessing services for those pupils who will not be using an automated biometric recognition system. The Trust will comply with any guidance or advice issued by the Department for Education on the use of Biometric Data from time to time.

5.10 The Trust and / or the relevant academies must obtain the explicit Consent of staff, trustees, local governors, members or other Data Subjects before Processing their Biometric Data.

6. CRIMINAL CONVICTIONS AND OFFENCES

6.1 There are separate safeguards in the UK GDPR for Personal Data relating to criminal convictions and offences.

6.2 It is likely that the Trust and its academies will Process Data about criminal convictions or offences. This may be as a result of pre-vetting checks we are required to undertake on staff, trustees and local governors or due to information which we may acquire during the course of their employment or appointment.

6.3 In addition, from time to time we may acquire information about criminal convictions or offences involving pupils or Parents. This information is not routinely collected and is only likely to be processed by the Trust in specific circumstances, for example, if a child protection issue arises or if a parent / carer is involved in a criminal matter.

6.4 Where appropriate, such information may be shared with external agencies such as the child protection team at the Local Authority, the Local Authority Designated Officer and / or the Police. Such information will only be processed to the extent that it is lawful to do so and appropriate measures will be taken to keep the data secure.

7. TRANSPARENCY

7.1 One of the key requirements of the UK GDPR relates to transparency. This means that the Trust must keep Data Subjects informed about how their Personal Data will be processed when it is collected.

7.2 One of the ways we provide this information to individuals is through a privacy notice which sets out important information what we do with their Personal Data. The Trust has developed privacy notices for the following categories of people:

7.2.1 Pupils, Parents & Carers

7.2.2 Staff, Trustees & Local Governors

7.3 The Trust wishes to adopt a layered approach to keeping people informed about how we process their Personal Data. This means that the privacy notice is just one of the tools we will use to communicate this information. Trust employees are expected to use other appropriate and proportionate methods to tell individuals how their Personal Data is being processed if Personal Data is being processed in a way that is not envisaged by our privacy notices and / or at the point when individuals are asked to provide their Personal Data, for example, where Personal Data is collected about visitors to Academy premises or if we ask people to complete forms requiring them to provide their Personal Data.

7.4 We will ensure that privacy notices are concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

8. CONSENT

8.1 The Trust must only process Personal Data on the basis of one or more of the lawful bases set out in the UK GDPR, which include Consent. Consent is not the only lawful basis and there are likely to be many circumstances when we process Personal Data and our justification for doing so is based on a lawful basis other than Consent.

8.2 A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

8.3 In the event that we are relying on Consent as a basis for Processing Personal Data about pupils, if a pupil is aged under 13, we will need to obtain Consent from the Parent(s). In the event that we require Consent for Processing Personal Data about pupils aged 13 or over, we will require the Consent of the pupil although, depending on the circumstances, academies should consider whether it is appropriate to inform Parents about this process. Consent is likely to be required if, for example,

an academy wishes to use a photo of a pupil on its website or on social media. Consent is also required is also required before any pupils are signed up to online learning platforms. Such Consent must be from the Parent is the pupil is aged under 13. When relying on Consent, we will make sure that the child understands what they are consenting to, and we will not exploit any imbalance in power in the relationship between us.

8.4 Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if we intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

8.5 Unless we can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data. Often we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data.

8.6 Evidence and records of Consent must be maintained so that the Trust can demonstrate compliance with Consent requirements.

9. SPECIFIED, EXPLICIT AND LEGITIMATE PURPOSES

9.1 Personal data should only be collected to the extent that it is required for the specific purpose notified to the Data Subject, for example, in the Privacy Notice or at the point of collecting the Personal Data. Any data which is not necessary for that purpose should not be collected in the first place.

9.2 The Trust will be clear with Data Subjects about why their Personal Data is being collected and how it will be processed. We cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have Consented where necessary.

10. ADEQUATE, RELEVANT AND LIMITED TO WHAT IS NECESSARY

10.1 The Trust will ensure that the Personal Data collected is adequate to enable us to perform our functions and that the information is relevant and limited to what is necessary.

10.2 In order to ensure compliance with this principle, the Trust will check records at appropriate intervals for missing, irrelevant or seemingly excessive information and may contact Data Subjects to verify certain items of data.

10.3 Trust employees must also give due consideration to any forms stakeholders are asked to complete and consider whether all the information is required. We may only collect Personal Data that is needed to operate as a school function and we should not collect excessive data. We should ensure

that any Personal Data collected is adequate and relevant for the intended purposes.

10.4 The Trust will implement measures to ensure that Personal Data is processed on a 'Need to Know' basis. This means that only members of staff, local governors or trustees who need to know Personal Data about a Data Subject will be given access to it and no more information than is necessary for the relevant purpose will be shared. In practice, this means that the Trust may adopt a layered approach in some circumstances, for example, members of staff, trustees or local governors may be given access to basic information about a pupil or employee if they need to know it for a particular purpose but other information about a Data Subject may be restricted to certain members of staff who need to know it, for example, where the information is Sensitive Personal Data, relates to criminal convictions or offences or is confidential in nature (for example, child protection or safeguarding records).

10.5 When Personal Data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with the Trust's data retention guidelines.

11. ACCURATE AND WHERE NECESSARY KEPT UP-TO-DATE

11.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

11.2 If a Data Subject informs the Trust of a change of circumstances their records will be updated as soon as is practicable.

11.3 Where a Data Subject challenges the accuracy of their data, the Trust will immediately mark the record as potentially inaccurate, or 'challenged'. In the case of any dispute, we shall try to resolve the issue informally, but if this proves impossible, disputes will be referred to the Data Protection Officer for their judgement. If the problem cannot be resolved at this stage, the Data Subject should refer their complaint to the Information Commissioner's Office. Until resolved the 'challenged' marker will remain and all disclosures of the affected information will contain both versions of the information.

11.4 Notwithstanding paragraph 11.3, a Data Subject continues to have rights under the UK GDPR and may refer a complaint to the Information Commissioner's Office regardless of whether the procedure set out in paragraph 11.3 has been followed.

12. DATA TO BE KEPT FOR NO LONGER THAN IS NECESSARY FOR THE PURPOSES FOR WHICH THE PERSONAL DATA ARE PROCESSED

12.1 Personal data should not be kept longer than is necessary for the purpose for which it is held. This means that data should be destroyed or erased from our systems when it is no longer required.

12.2 It is the duty of the DPO, after taking appropriate guidance for legal considerations, to ensure that obsolete data are properly erased. The Trust has a retention schedule for all data.

13. DATA TO BE PROCESSED IN A MANNER THAT ENSURES APPROPRIATE SECURITY OF PERSONAL DATA

13.1 The Trust has taken steps to ensure that appropriate security measures are taken against unlawful or unauthorised processing of Personal Data, and against the accidental loss of, or damage to, Personal Data. Data Subjects may apply to the courts for compensation if they have suffered damage from such a loss.

13.2 The UK GDPR requires us to put in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

13.3 We will develop, implement and maintain safeguards appropriate to our size, scope, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

13.4 Data Users are responsible for protecting the Personal Data we hold. Data Users must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. Data Users must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

13.5 Data Users must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. Data Users must comply with all applicable aspects of our Data Security and E-Safety policies and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the UK GDPR and relevant standards to protect Personal Data.

13.6 Data Users must be aware that it is a criminal offence for someone to knowingly or recklessly obtain or disclose Personal Data without the Trust's consent (or to ask someone to do it on their behalf) and / or to retain it without our knowledge (for example, if a member of staff accesses Personal Data

about pupils or other members of staff without our consent and / or shares that data with people who are not permitted to see it). It is also an offence to sell or try to sell such Personal Data. These offences will also be treated as disciplinary issues in accordance with the Trust's HR policies.

13.7 Maintaining data security means guaranteeing the confidentiality, integrity and availability of the Personal Data, defined as follows:

13.7.1 Confidentiality means that only people who are authorised to use the data can access it.

13.7.2 Integrity means that Personal Data should be accurate and suitable for the purpose for which it is processed.

13.7.3 Availability means that authorised users should be able to access the data if they need it for authorised purposes.

13.8 It is the responsibility of all members of staff, trustees and local governors to work together to ensure that the Personal Data we hold is kept secure. We rely on our colleagues to identify and report any practices that do not meet these standards so that we can take steps to address any weaknesses in our systems. Anyone who has any comments or concerns about security should notify the Headteacher of the relevant School, Deputy DPO or the Internal or External DPO.

14. PROCESSING IN LINE WITH DATA SUBJECTS' RIGHTS

14.1 This information is detailed within the Privacy Notice.

15. SUBJECT ACCESS REQUESTS

15.1 This information is detailed in the Privacy Notice.

16. AUTHORISED DISCLOSURES

16.1 The Trust will only disclose data about individuals if one of the lawful bases apply.

16.2 Only authorised and trained staff are allowed to make external disclosures of Personal Data. The Trust and its academies will regularly share Personal Data with third parties where it is lawful and appropriate to do so including, but not limited to, the following:

16.2.1 Local Authorities

16.2.2 the Department for Education

16.2.3 the Catholic Education Service

16.2.4 the Education & Skills Funding Agency

16.2.5 the Diocese of Westminster

16.2.6 the Disclosure and Barring Service

16.2.7 the Local Safeguarding Board relevant to the Academies location

16.2.8 the Teaching Regulation Agency

16.2.9 the Teachers' Pension Service

16.2.10 the Local Government Pension Scheme which is administered by Hertfordshire, Hillingdon, Hounslow and Brent Pension Scheme Administrators for our academies depending on their location

16.2.11 our external HR providers

16.2.12 OfSTED

16.2.13 our external auditors

16.2.14 our external payroll providers

16.2.15 our external IT Providers

16.2.16 HMRC

16.2.17 the Police or other law enforcement agencies

16.2.18 our legal advisors and other consultants

16.2.19 insurance providers / the Risk Protection Arrangement

16.2.20 occupational health advisors

16.2.21 exam boards including AQA, OCR, Edexcel, WJEC, BTEC,

16.2.22 the Joint Council for Qualifications;

16.2.23 the Standards and Testing Agency;

16.2.24 NHS health professionals including educational psychologists and school nurses;

16.2.25 Education Welfare Officers;

16.2.26 Courts, if ordered to do so;

16.2.27 Prevent teams in accordance with the Prevent Duty on schools;

16.2.28 other schools, for example, if we are negotiating a managed move and we have Consent to share information in these circumstances;

16.2.29 confidential waste collection companies;

16.3 Some of the organisations we share Personal Data with may also be Data Controllers in their own right in which case we will be jointly controllers of Personal Data and may be jointly liable in the event of any data breaches.

16.4 Data Sharing Agreements should be completed when setting up 'on-going' or 'routine' information sharing arrangements with third parties who are Data Controllers in their own right. However, they

are not needed when information is shared in one-off circumstances but a record of the decision and the reasons for sharing information should be kept.

16.5 All Data Sharing Agreements must be signed off by the School Deputy DPO who will keep a register of all Data Sharing Agreements.

16.6 The UK GDPR requires Data Controllers to have a written contract in place with Data Processors which must include specific clauses relating to the way in which the data is Processed ("UK GDPR clauses"). A summary of the UK GDPR clauses is set out in Appendix 1. It will be the responsibility of the Academy entering into the contract to ensure that the UK GDPR clauses have been added to the contract with the Data Processor. Personal data may only be transferred to a third-party Data Processor if they agree to put in place adequate technical, organisational and security measures themselves.

16.7 In some cases Data Processors may attempt to include additional wording when negotiating contracts which attempts to allocate some of the risk relating to compliance with the UK GDPR, including responsibility for any Personal Data Breaches, onto the Trust. In these circumstances, the member of staff dealing with the contract should contact the Internal or External DPO for further advice before agreeing to include such wording in the contract.

17. ACCOUNTABILITY

17.1 The Trust must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Trust is responsible for, and must be able to demonstrate, compliance with the data protection principles.

17.2 The Trust must have adequate resources and controls in place to ensure and to document UK GDPR compliance including:

17.2.1 appointing a suitably qualified DPO (where necessary) and an executive team accountable for data privacy;

17.2.2 implementing Privacy by Design when Processing Personal Data and completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;

17.2.3 integrating data protection into internal documents including this Data Protection Policy, related policies and Privacy Notices;

17.3 regularly training Trust employees, trustees and local governors on the UK GDPR, this Data Protection Policy, related policies and data protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The Trust must maintain a record of training attendance by Trust personnel; and regularly testing the privacy measures implemented and

conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

18. RECORD KEEPING

18.1 The UK GDPR requires us to keep full and accurate records of all our Data Processing activities.

18.2 We must keep and maintain accurate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents.

18.3 These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

19. TRAINING AND AUDIT

19.1 We are required to ensure all Trust personnel have undergone adequate training to enable us to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

19.2 Members of staff must attend all mandatory data privacy related training.

20. PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

20.1 We are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

20.2 This means that we must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

20.2.1 the state of the art;

20.2.2 the cost of implementation;

20.2.3 the nature, scope, context and purposes of Processing; and

20.2.4 the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

20.3 We are also required to conduct DPIAs in respect to high risk processing.

20.4 The Trust and its academies should conduct a DPIA and discuss findings with the DPO when implementing major system or business change programs involving the Processing of Personal Data including (but not limited to):

20.4.1 use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

20.4.2 Automated Processing including profiling and ADM;

20.4.3 large scale Processing of Sensitive Data; and

20.4.4 large scale, systematic monitoring of a publicly accessible area.

20.5 We will also undertake a DPIA as a matter of good practice to help us to assess and mitigate the risks to pupils. If our processing is likely to result in a high risk to the rights and freedom of children then a DPIA should be undertaken.

20.6 A DPIA must include:

20.6.1 a description of the Processing, its purposes and the Trust's legitimate interests

20.6.2 an assessment of the necessity and proportionality of the Processing in relation to its purpose

20.6.3 an assessment of the risk to individuals

20.6.4 the risk mitigation measures in place and demonstration of compliance

21. CCTV

21.1 The Trust and its academies use CCTV in locations around their sites. This is to:

21.1.1 protect the academy buildings and their assets;

21.1.2 increase personal safety and reduce the fear of crime;

21.1.3 support the Police in a bid to deter and detect crime;

21.1.4 assist in identifying, apprehending and prosecuting offenders;

21.1.5 provide evidence for the Trust to use in its internal investigations and / or disciplinary processes in the event of behaviour by staff, pupils or other visitors on the site which breaches or is alleged to breach the Trust's policies;

21.1.6 protect members of the school community, public and private property; and

21.1.7 assist in managing the academy.

21.2 Please refer to the School's CCTV policy for more information.

22. WHAT IS A PERSONAL DATA BREACH?

22.1 The legal definition of a personal data breach is, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."

22.2 A data security breach covers more than the simple misappropriation of data and may occur through incidents, such as:

22.2.1 Loss or theft of data or equipment;

22.2.2 People gaining inappropriate access to personal data;

22.2.3 A deliberate attack on systems;

22.2.4 Equipment failure;

22.2.5 Human error;

22.2.6 Acts of God (for example, fire or flood);

22.2.7 Malicious acts such as hacking, viruses or deception.

22.3 Breaches can be categorised according to the following three well-known information security principles:

22.3.1 "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data;

22.3.2 "Integrity breach" - where there is an unauthorised or accidental alteration of personal data;

22.3.3 "Availability breach" - where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

22.4 Depending on the circumstances, a breach can relate to the confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

22.5 A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

22.6 A security incident resulting in personal data being made unavailable for temporary period is also a type of breach, as the lack of access to the data could have a significant impact on the rights and freedoms of data subjects, for example, if our IT system goes down. This type of breach should be recorded in the School's Data Breach Log (within the electronic UK GDPR folder). However, depending on the circumstances of the breach, it may or may not require notification to the ICO and communication to affected individuals.

22.7 Where personal data is unavailable due to planned system maintenance being carried out, this should not be regarded as a 'breach of security'.

23. UNDERSTANDING THE RISKS TO THE RIGHTS AND FREEEDOMS OF INDIVIDUALS

23.1 A breach can potentially have a number of consequences for individuals, which can result in physical, material, or non-material damage. This can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals.

23.2 When assessing the risk to individuals, the External Trust DPO , Internal DPO (and school-based internal Deputy DPO) will consider the following factors:

23.2.1 the type of breach;

23.2.2 the nature, sensitivity, and volume of personal data;

23.2.3 ease of identification of individuals;

23.2.4 severity of consequences for individuals;

23.2.5 special characteristics of the individual;

23.2.6 special characteristics of the data controller; and

23.2.7 the number of affected individuals.

24. TIMESCALES FOR REPORTING A BREACH

24.1 The School is required to report a notifiable breach without undue delay and, where feasible, not later than 72 hours after having become aware of it.

24.2 It is likely that the school will be deemed as having become “aware” of a breach when there is a reasonable degree of certainty that a security incident has occurred which has led to personal data being compromised. The UK GDPR expects us to ascertain whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place. This puts an obligation on us to ensure that we will be “aware” of any breaches in a timely manner so that we can take appropriate action.

24.3 While some breaches may be obvious, in other cases we may need to establish whether personal data has been compromised. In such circumstances, we will investigate promptly in accordance with the procedures below to determine whether a breach has happened which, in turn, will enable us to decide if remedial action is needed and if the breach needs to be notified to the ICO and the affected data subjects.

24.4 It is possible that we may not have established all of the relevant facts following a data security breach

or completed our investigation within 72 hours. However, in the event that the school determines that a breach has taken place and that it needs to be notified to the ICO, a report should be made within 72 hours with the information held at that point in time. In these circumstances, the report to the ICO should explain that further information will be provided as and when it is available.

24.5 It is possible that some breaches may come to the attention of a member of staff or may be flagged up by our IT systems. However, it is also possible that we may be notified about breaches by third parties, such as the people who are affected by the breach, a data processor or by the media.

24.6 In the event that we investigate a suspected breach and we are able to establish that no actual breach has occurred, the Data Breach Log must still be updated so that we can keep records of 'near misses' or other weaknesses in our systems and procedures in order to continuously review and improve our processes.

25. RESPONSE PLAN AND CONTACT DETAILS

25.1 An individual who becomes aware of a suspected or actual data security breach, must inform the Headteacher and the Internal School Deputy DPO (detailed in the individual school Privacy Notice), or the Trust External and Internal DPO without delay. The Internal Trust DPO can be contacted via the 'Contact Us' form on the Trust website https://www.dowat.co.uk/148/contact-us-1 or at dpo@dowat.co.uk

25.2 If a member of staff is unsure if a breach has happened, the above procedures must still be followed without delay so that the suspected breach can be investigated to establish whether a breach has happened and, if so, whether it needs to be notified to the ICO or the data subjects.

25.3 The School Deputy DPO, will then be responsible for assessing whether the breach or suspected breach needs to be formally escalated to the Trust DPO. If the Deputy DPO decides not to escalate it to the Trust DPO, the Data Breach Log must be completed as accurately as possible, including the reasons why the incident does not need to be escalated to the Trust DPO. The Data Breach Log is reviewed by the Trust DPO termly.

25.4 If the Deputy DPO decides to escalate a breach or suspected breach to the Trust DPO, they must do so without delay. Where possible, an entry in the Data Breach Log must be completed with as much information as possible. However, if it is not convenient or practicable to complete the Data Breach Log, the report can be made by setting the information out in an email or over the phone in extreme cases, though a written record is required.

25.5 Once a breach or suspected breach has been reported to the Trust DPO, or School Deputy DPO, an investigation must commence to assess whether there is sufficient information to identify next steps. The purpose of the investigation is to:

25.5.1 establish if a breach has happened;

25.5.2 establish the nature and cause of the breach;

25.5.3 establish the extent of the damage or harm that results or could result from the breach;

25.5.4 identify the action required to stop the data security breach from continuing or recurring; and

25.5.5 mitigate any risk of harm that may continue to result from the breach.

25.6 The Deputy or Trust DPO will contact the Headteacher if further information is required. The Deputy or Trust DPO may also need to speak to the member of staff who first reported the breach or suspected breach.

25.7 During the course of their investigation, the Deputy DPO should consider whether to involve the School's Data Breach Response Team which consists of:

25.7.1 Headteacher and Deputy or Trust DPO as required, plus other staff at the Headteacher's request.

25.7.2 School Business Manager or another member of SLT (as appropriate),

25.7.3 If the Trust DPO is unavailable for any reason, Deputy DPO must fulfil the responsibilities of the Trust DPO set out in this Data Breach Response Plan.

25.8 If the Deputy or Trust DPO decides to involve the Data Breach Response Team, the above individuals will be copied into email correspondence and provided with regular updates on the investigation and response to the incident.

25.9 Either DPO should consider whether input is required (e.g. from School IT or HR teams) in order to further investigate the incident, including the extent of the incident and whether any steps need to be taken to contain any breach. Contact details for IT support are available in the office.

25.10 Depending on the circumstances, the Trust DPO should consider whether the insurers should be notified in accordance with policy terms, whether legal advice is required and if the incident needs to be reported to the Police. One of the DPOs will also consider if specialist IT support is required in order to contain and manage a breach and whether dedicated PR or communications support should be engaged if it is likely that communication internally and / or externally with stakeholders regarding the breach or suspected breach is required.

25.11 If the breach or suspected breach has occurred by one of our Data Processors, the DPO must liaise with the Data Processor to obtain as much information as possible about the extent of the breach or suspected breach and any steps being taken to mitigate any risk to data subjects. It remains the school's responsibility along with guidance from the DPO, to decide whether to report any such breach to the ICO within 72 hours.

25.12 The same requirement applies if the breach or suspected breach is reported to us by a joint Data Controller, though in this case the school/Trust should establish with the joint Data Controller who will

report the breach to the ICO and the data subjects, if the threshold is reached.

25.13 Depending on the timescales as to when a member of staff originally became aware of a breach, the DPO must be mindful of the requirement to notify the ICO (if necessary) without delay and within 72 hours unless it is unlikely to result in a risk to the rights and freedoms of individuals. It is therefore possible that a data security breach may need to be reported to the ICO before a full investigation has occurred, and during breach containment, rather than after. A report to the ICO must contain the following information:

25.13.1 the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned;

25.13.2 the name and contact details of the Trust DPO/Deputy DPO or other contact point where more information can be obtained;

25.13.3 the likely consequences of the personal data breach;

25.13.4 the measures taken or proposed to be taken by the school/Trust to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

25.14 The Trust DPO or Deputy DPO is not required to provide precise details in the report to the ICO if this information is not available, and an updated report can be made as and when further details come to light. Such further information may be provided in phases without undue further delay. The Trust DPO or Deputy DPO should inform the ICO if the school does not yet have all the required information and if further details will be provided later on.

25.15 If a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred, this information could then be added to the information already given to the ICO and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

25.16 In the event that a notifiable breach is not reported to the ICO within 72 hours, a report should be made without delay, detailing the reasons for the delay.

25.17 If the DPO concludes that a referral to the ICO is required and also concludes that there is likely to be a high risk to the rights and freedoms of individuals resulting from the data security breach then the data subjects affected by the breach must also be notified without undue delay. The Trust DPO or Deputy DPO will liaise with the Headteacher in relation to how the issue should be communicated to the relevant stakeholders. The school should consider which is the most appropriate way to notify affected data subjects, bearing in mind the security of the medium as well as the urgency of the situation. The notice to the affected individuals should contain the following information:

25.17.1 description of the nature of the breach

25.17.2 the name and contact details of the DPO or other contact point

25.17.3 a description of the likely consequences of the breach

25.17.4 a description of the measures taken or proposed to be taken by the school/Trust to address the breach, including, where appropriate, measures to mitigate its possible adverse effects

25.18 Given that a large number of our stakeholders are children, if a data breach affects our pupils, the above information may need to be given to parents / carers for affected pupils who are aged 13 or under.

25.19 If the DPO decides to notify data subjects about a breach, the notification should at the very least include a description of how and when the breach occurred and what data was involved. Details of what the organisation has already done to respond to the risks posed by the breach should also be included. The school should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised.

25.20 The DPO must complete the Data Breach Log before making the referral to the ICO and keep it under review as and when further information comes to light.

25.21 In certain circumstances, where justified, and on the advice of law-enforcement authorities, the school may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

25.22 Even if the DPO initially decides not to communicate the breach to the affected data subjects, the ICO can require us to do so, if it considers the breach is likely to result in a high risk to individuals.

25.23 In the event that the DPO concludes that it is not necessary to refer the breach to the ICO, the Deputy DPO must still complete the Data Breach Log and clearly set out the reasons why the Trust DPO or Deputy DPO is satisfied that a referral is not required. The school must keep the decision under review and prepare to make a referral to the ICO if any circumstances change, or if any information comes to light which means that a referral should be made.

25.24 Once the breach has been contained and action taken to stop or mitigate the breach, the Deputy DPO or DPO must then review the incident and identify any steps which need to be taken in order to prevent a similar breach occurring in future. This may also include whether any disciplinary action is required against any members of staff or pupils.

25.25 As part of the review process, the school should undertake an audit which should include a review of whether appropriate security policies and procedures were in place and if so, whether they were followed. The audit should include an assessment of any ongoing risks associated with the breach and evaluate the school response to it and identify any improvements that can be made. The review should also consider the effectiveness of this Data Breach Response Plan and whether any

amendments need to be made to it.

25.26 Where security is found not to be appropriate, the DPO should consider what action needs to be taken to raise data protection and security compliance standards and whether any staff training is required.

25.27 Where a data processor caused the breach, the DPO should consider whether adequate contractual obligations were in place to comply with the UK GDPR and if so, whether the data processor is in breach of contract.

26. RECORD KEEPING

26.1 Record Keeping logs will be kept according to the school Privacy Notices.

26.2 The Internal Trust DPO checks processes and controls at least annually and logs of Data Risk, Data Breaches, Subject Access Requests are maintained by the school and subject to inspection and interrogation during Trust DPO inspections.

27. SCHOOL HOLIDAYS

27.1 The Trust recognises that there are times throughout the year when our ability to identify and respond to a breach swiftly and robustly may be impeded because the school is closed and has limited staff available during school holidays. A breach may still occur during these periods and we will implement the following steps to mitigate any risk caused if a breach happens during the school holidays:

27.1.1 The email address dpo@dowat.co.uk is available on our website and in our privacy notices so that a member of staff can be contacted should an incident occur. This email address will be monitored regularly by the assigned member of staff.

27.1.2 The Internal Trust DPO and Deputy School DPO will have the contact details for the Headteacher and IT support so that action can be taken without delay should a breach occur.

27.1.3 The DPO should follow the steps set out above as best as they can in the circumstances. In particular, this should include reporting notifiable breaches to the ICO within 72 hours and, if required, the affected individuals. The report to the ICO should state that the school is closed and has limited staff available due to the school holidays and, depending on the circumstances, advice should be sought from the ICO on the steps the school should take to mitigate any risks.

28. REVIEW

28.1 This Data Breach Response Plan will be kept under review by the Internal Trust DPO and may be revised to reflect good practice or changes to our organisational structure.

29. HOW DO WE PROTECT OUR DATA?

29.1 Our data backup and security measures are documented in the Supplier Compliance Evidence folder; part of the UK GDPR folder within the school central electronic filing system, accessible by senior and key support staff.. This organisation responsible for data backup has detailed the current security measures and storage processes/methods. Any changes to this system or procedure will be evident by an updated version number of that document.

30. ANTI-FRAUD SUPPORT

30.1 The Anti-Fraud Service for our schools is set out below:

Hertfordshire	0300 123 4033 fraud.team@hertfordshire.gov.uk www.hertfordshire.gov.uk/fraud
Hillingdon	0800 389 8313
Brent	020 89371279 investigations@brent.gov.uk
Hounslow	0800 328 6453 fraud@hounslow.gov.uk

APPENDIX 1

30.2 The UK GDPR requires the following matters to be addressed in contracts with Data Processors. The wording below is a summary of the requirements in the UK GDPR and is not intended to be used as the drafting to include in contracts with Data Processors.

1. The Processor may only process Personal Data on the documented instructions of the controller, including as regards international transfers. (Art. 28(3)(a))
2. Personnel used by the Processor must be subject to a duty of confidence. (Art. 28(3)(b))
3. The Processor must keep Personal Data secure. (Art. 28(3)(c) Art. 32)
4. The Processor may only use a sub-processor with the consent of the Data Controller. That consent may be specific to a particular sub-processor or general. Where the consent is general, the processor must inform the controller of changes and give them a chance to object.(Art. 28(2) Art. 28(3)(d))

30.3 The Processor must ensure it flows down the UK GDPR obligations to any sub-processor. The Processor remains responsible for any processing by the sub-processor. (Art. 28(4))

5. The Processor must assist the controller to comply with requests from individuals exercising their rights to access, rectify, erase or object to the processing of their Personal Data. (Art. 28(3)(e))
6. The Processor must assist the Data Controller with their security and data breach obligations, including notifying the Data Controller of any Personal Data breach. (Art. 28(3)(f)) (Art. 33(2))
7. The Processor must assist the Data Controller should the Data Controller need to carry out a privacy impact assessment. (Art. 28(3)(f))
8. The Processor must return or delete Personal Data at the end of the agreement, save to the extent the Processor must keep a copy of the Personal Data under Union or Member State law. (Art. 28(3)(g))
9. The Processor must demonstrate its compliance with these obligations and submit to audits by the Data Controller (or by a third party mandated by the controller). (Art. 28(3)(h))

30.4 The Processor must inform the Data Controller if, in its opinion, the Data Controller's instructions would breach Union or Member State law. (Art. 28(3)).