

|                                     |                                                                                                  |
|-------------------------------------|--------------------------------------------------------------------------------------------------|
| <b>Policy Title:</b>                | Data Protection                                                                                  |
| <b>Version:</b>                     | 1.3                                                                                              |
| <b>Member of Staff Responsible:</b> | Chief Executive Officer                                                                          |
| <b>Status:</b>                      | Statutory                                                                                        |
| <b>Date adopted by Trust Board:</b> | 13 <sup>th</sup> October 2025                                                                    |
| <b>Date for Review:</b>             | September 2026                                                                                   |
| <b>Reviewed:</b>                    | 9 <sup>th</sup> December 2021<br>11 <sup>th</sup> December 2023<br>14 <sup>th</sup> October 2024 |

| Change Record |            |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Version       | Date       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 1.1           | 13/12/23   | Amendments to Section 5.2, 18                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 1.2           | 14/10/24   | Amendments to 5.2 change of DPO<br>Amendments to Section 8, 9.1, 12, 13, 16, 18, 19, 21<br>New Section 11 on Biometric Recognition systems,<br>Section 14 on AI and AI Protocol Appendix 3<br>Introduction of Appendix 4 SAR procedure                                                                                                                                                                                                          |
| 1.3           | 26/09/2025 | Amendment to section 9.1 & 9.3 to confirm any search for data under a SAR will be reasonable and proportionate. Section 9.3 updated to include requests during academy closure periods.<br>Appendix 4 renumbered to Appendix 3 with the deletion of the AI protocol<br>Amendment to section 14 references the new Trust AI Governance Framework and deletion of Appendix 3 AI protocol.<br>Addition of data protection complaints in section 20 |
| 1.4           |            |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

**Primitas Learning Partnership promotes the safeguarding and welfare of all children in its care;  
all policies are developed and formulated with this in mind**

## DATA PROTECTION POLICY

### 1. Aims

Our Trust, Primitas Learning Partnership("Primitas") aims to ensure that all personal data collected about staff, students, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (UK GDPR) and the provisions of the Data Protection Act 2018 (DPA 2018) and the Data Use and Access Act (DUAA 2025).

This policy applies to all personal data, regardless of whether it is in paper or electronic format.

### 2. Legislation and guidance

This policy meets the requirements of the UK GDPR and the expected provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

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

In addition, this policy complies with our funding agreement and articles of association.

### 3. Definitions

| Term                                       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Personal data</b>                       | <p>Any information relating to an identified, or identifiable, living, individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"><li>• Name (including initials)</li><li>• Identification number</li><li>• Location data</li><li>• Online identifier, such as a username</li></ul> <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity.</p>               |
| <b>Special categories of personal data</b> | <p>Personal data which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"><li>• Racial or ethnic origin</li><li>• Political opinions</li><li>• Religious or philosophical beliefs</li><li>• Trade union membership</li><li>• Genetics</li><li>• Biometrics (such as fingerprints, retina and iris patterns), where used for identification purposes</li><li>• Health – physical or mental</li></ul> |

|                             |                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | <ul style="list-style-type: none"> <li>• Sex life or sexual orientation</li> <li>• Safeguarding</li> <li>• Additional Needs Information</li> </ul>                                                                   |
| <b>Processing</b>           | 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. |
| <b>Data subject</b>         | The identified or identifiable individual whose personal data is held or processed.                                                                                                                                  |
| <b>Data controller</b>      | A person or organisation that determines the purposes and the means of processing of personal data.                                                                                                                  |
| <b>Data processor</b>       | A person or other body, other than an employee of the data controller, who processes personal data on behalf of the data controller.                                                                                 |
| <b>Personal data breach</b> | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.                                                                    |

#### 4. The Data Controller(s)

Primitas is registered as a Data Controller with the ICO. Individual Academies are listed under the Primitas registration as they are the Data Controllers for the data that the Academy holds. This registration will be renewed annually or as otherwise legally required.

#### 5. Roles and Responsibilities

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

##### 5.1 Trust Board

The Board of Trustees is ultimately accountable for how personal information is handled and has overall responsibility for ensuring that Primitas complies with all relevant data protection laws. The Chief Executive Officer is not a Trustee, but works for and behalf of the Trust Board on a day-to-day basis to ensure that Data Protection obligations are met.

##### 5.2 Data Protection Officer

The Data Protection Officer (DPO) for Primitas is Jackie Hesslegrave and is contactable via [DPO@primitas.co.uk](mailto:DPO@primitas.co.uk). It is the responsibility of the DPO to oversee the implementation of this policy and develop related policies and guidelines where applicable to enable the Trust to comply with data

protection law. The DPO will report to the highest level of management which is the Chief Executive Officer.

Each individual academy will have a Data Protection Lead (DPL) who will lead on Data Protection issues locally and will be advised by, and work closely with the DPO.

They will regularly report their activities directly to the Local Governing Body and, where relevant, report to the Trust Board advice and recommendations on school data protection issues in local schools.

The DPO and works proactively with DPLs to help them:

- Keep up to date with data protection developments
- Raise awareness of data protection priorities in their academy
- Monitor data protection compliance

All queries concerning data protection matters should be raised with the academy's DPL in the first instance, who will liaise with the DPO as required.

The Data Protection Lead will also report to the Local Governing Body about their activity and any pertinent data protection issues in the local academy.

### **5.3 Headteachers**

The Headteacher of each academy acts as the representative of the Data Controller on a day-to-day basis and works with the DPL to raise awareness, provide training and updates, check compliance and maintain vigilance in matters of data protection at local level.

### **5.4 All staff**

Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address
- Contacting the DPO in the following circumstances:
  - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
  - If they have any concerns that this policy is not being followed
  - If they are unsure whether or not they have a lawful basis to use personal data in a particular way
  - If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK
  - 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

## **6. Data protection principles**

The UK GDPR is based on data protection principles that our school must comply with.

The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes

- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

## 7. Collecting personal data

### 7.1 Lawfulness, fairness and transparency

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

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

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

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

### 7.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary.

Staff must only process personal data where it is necessary in order to do their jobs. When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Documentation Retention Policy.

## 8. Sharing personal data

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

- There is an issue with a student or parent/carer that puts the safety of our staff at risk
- We need to liaise with other agencies – we will seek consent as necessary before doing this
- Our suppliers or contractors need data to enable us to provide services to our staff and students – for example, IT companies. When doing this, we will:

- Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
- Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
- Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for:

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

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

Where we transfer personal data to another country we will do so in accordance with UK data protection law.

## **9. Subject access requests and other rights of individuals**

### **9.1 Subject access requests**

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

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

To avoid ambiguity subject access requests should be submitted in writing, either by letter, email to the DPL. They should include:

- Name of individual
- Correspondence address
- Contact number and email address
- Details of the information requested
- How the individual would like the information to be given to them, e.g. hard copy in person via post, electronic copy via email

If a request is not submitted in writing the Data Protection Lead will contact the requestor to obtain the above information.

Dependent upon the amount of data held on a subject and to make a proportionate and reasonable search for data during a subject access request, the DPL may return to the requestor and ask them to narrow their request and be more specific about the data they are requesting. Should this occur, the clock will stop whilst this clarification is sought, and the timeframe for responding adjusted accordingly. Should the requestor not provide clarification the Academy will determine what is reasonable and proportionate with support from the DPO.

If staff receive a subject access request they must immediately inform the Data Protection Lead within their setting who will liaise with the DPO. The SAR procedure is detailed in Appendix 3.

## **9.2 Children and subject access requests**

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

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

## **9.3 Responding to subject access requests**

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual we will comply within 3 months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month, and explain why the extension is necessary
- Will conduct a reasonable and proportionate search for data

### **Requests affected by school closure periods**

Requests received during Academy/Trust closure periods may not be able to be responded to within one calendar month response period. This is because the Academy/Trust will be closed and no one will be on site to comply with the request. As a result, it is unlikely that a request will be able to be dealt or acknowledged during this time. The Academy/Trust will endeavour to comply with requests as soon as possible and will keep in communication with you as far as possible. If your request is urgent, please provide your request during term times and not during / close to closure periods.

We will not disclose information if it:

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

- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee which takes into account administrative costs.

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

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

#### **9.4 Other data protection rights of the individual**

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the UK
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- Be notified of a data breach in certain circumstances
- Make a complaint to the ICO
- Ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format (in certain circumstances)

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

#### **10. Parental requests to see the educational record**

Parents, or those with parental responsibility, may request access to their child's educational record (which includes most information about a student) within 15 school days of receipt of a written request. Requests should be made via school office address.

#### **11. Biometric recognition systems**

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

Parents or those with parental responsibilities will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least 1 parent or person with parental responsibility before we take any biometric data from their child and first process it.

Parents or those with parental responsibility and students have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

Parents or those with parental responsibility and students can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

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

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

## **12. CCTV**

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

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

Any enquiries about the CCTV system in our Academies should be directed to the Headteacher.

## **13. Photographs and videos**

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

We will obtain written consent from parents/carers, or students aged 18 and over, for photographs and videos to be taken of students for communication, marketing and promotional materials.

Uses may include:

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

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

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

See our Safeguarding Policy and the individual Academy's Taking and Use of Images Policy for more information on our use of photographs and videos.

## **14. Artificial Intelligence (AI)**

Artificial intelligence (AI) tools are now widespread and easy to access. They provide computer generated answers to queries a user may pose or provide computer generated tasks that would previously require human intelligence. Staff, students and parents or those with parental responsibility may be familiar with generative chatbots such as ChatGPT, Copilot, or Google Gemini. The Trust recognises that AI has many uses to help students learn, but also poses risks to sensitive and personal data. Specific risks are recognised as:

- The answer to a query may be incorrect
- It may give inconsistent answers when asked the same question more than once
- May provide outdated information
- May provide information that is biased or discriminatory
- Create a security or data protection risk when confidential information is inputted

To ensure that personal and sensitive data remains secure, no one will be permitted to enter such data into unauthorised generative AI tools or chatbots.

In addition, staff may not input any information into AI tools or platforms that would identify the Trust or individual Academy.

If personal and/or sensitive data is entered into an unauthorised generative AI tool, The Trust will treat this as a data breach, and will follow the personal data breach procedure outlined in appendix 1.

Examples of confidential or sensitive information includes but is not limited to:

- Information about employees
- Information about students, parents, staff, suppliers, educational partners
- Financial information
- Internal policies and procedures

Staff members are responsible for the quality and accuracy of their work whilst AI can improve efficiency and productivity it should not be seen as a replacement for human judgement or expertise.

The Trust's protocol for use of AI is detailed in the Trust AI Governance Framework.

## **15. Data Protection and storage of records by design and default**

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices

- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of our processing activities, including:
  - For the benefit of data subjects, making available the name and contact details of our academies and 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, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

## **16. Data security and storage of records**

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

In particular:

- Paper-based documents and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Paper-based documents containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access
- Where paper-based documents containing personal information needs to be taken off site, staff are responsible for them and must ensure that they are kept safe and secure and not left anywhere with general access
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.
- Encryption software is used to protect all Trust and Academy portable devices and removable media, such as laptops and USB devices.
- Staff, students or governors must not store personal information on their personal devices unless the same stringent security procedures, as for school-owned equipment are followed (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 (see section 8)
- All virtual meetings will follow the guidelines set out in the Remote Meeting Protocols as found in Appendix 2

## **17. Disposal of records**

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where we cannot or do not need to rectify or update it.

For example, we will shred or incinerate paper-based records, and overwrite or delete electronic files. We may also use a third party to safely dispose of records on the school'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**

The Trust and individual academies will make all reasonable endeavours to ensure that there are no personal data breaches.

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

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

- A non-anonymised dataset being published on the school website which shows the exam results of students eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about students
- A cyber security incident

## **19. Training**

All staff, Trustees and Governors are provided with data protection and cyber security training as part of their induction process.

Data protection and cyber security awareness will also form part of continuing professional development, where changes to legislation, guidance or the academies' processes make it necessary.

## **20. Data Protection Complaints**

Should an individual have a complaint about the way their personal data has been used they are able to make a complaint by emailing [dpo@primitas.co.uk](mailto:dpo@primitas.co.uk). They will be required to complete a form which gives the full details of the complaint. The complaint will be acknowledged within 30 working days and responded to 'without undue delay'. Should an individual be dissatisfied with the outcome of their complaint they will be able to complain to the ICO.

## **21. Monitoring arrangements**

The DPO is responsible for monitoring and reviewing this policy.

The UK GDPR and the EU UK GDPR was incorporated into UK Legislation with some amendments in The Data Protection Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 and this policy has been amended to reflect these amendments.

This policy will be reviewed and updated if necessary when the Data Protection and Digital Information Bill receives royal assent and becomes law, if any changes are made to the bill that affect our practice. Otherwise, or from then on, this policy will be reviewed **every year** and shared with the full Governing Body.

## **22. Links with other policies**

This data protection policy is linked to our:

- Freedom of information publication scheme

- E-Safety Policy
- Safeguarding Policy
- Individual Academy Taking & Use of Images Policy
- Documentation Retention policy

## 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 Academy Data Protection Lead (DPL). The DPL will document the details on a Trust Data Breach form and notify the Trust Data Protection Officer (DPO).
- The DPO will investigate the report, and determine whether a breach has occurred. To decide, 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 Headteacher and the Chair of Governors
- The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant DPL 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 work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
  - Loss of control over their data
  - Discrimination
  - Identify theft or fraud
  - Financial loss
  - Unauthorised reversal of pseudonymisation (for example, key-coding)
  - Damage to reputation
  - Loss of confidentiality
  - Any other significant economic or social disadvantage to the individual(s) concernedIf it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Academy's computer system.
- 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 the Academy's computer system.
- The DPO, headteacher and DPL will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

### **Actions to minimise the impact of data breaches**

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)**

- All emails containing special category data (sensitive information) will be marked strictly confidential in the email title, even if these are being sent internally.
- Emails sending special category data (sensitive information) are to be encrypted.
- Attachments containing special category data are to be password protected and the password sent by separate email.
- 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 the ICT department 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

Other types of breach could include:

- Details of student premium interventions for named children being published on the school website
- Non-anonymised student exam results or staff pay information being shared with governors
- A school laptop containing non-encrypted sensitive personal data being stolen or hacked
- The school's cashless payment provider being hacked and parents' financial details stolen

## **APPENDIX 2**

### **Protocols for Virtual Meetings**

#### ***Meeting Platform: Microsoft Teams***

- If you cannot attend the whole of the meeting, inform the relevant person(s) beforehand, as you would for a face-to-face meeting.
- Logon to the meeting 5 minutes before the start time.
- Attend the meeting with video camera and microphone turned on until the meeting starts.
- Once the meeting starts, switch off the microphone to reduce interference.
- Remain on mute unless speaking.
- Be mindful of your surroundings and of the need for privacy/confidentiality. Therefore, wherever possible:
  - Ensure that you are in a room on your own.
  - Use headphones to limit the amount of information that is overheard by others.
  - Never undertake meetings in a public area e.g. cafes, parks etc.
  - Check your background thoroughly and ensure that no data is visible on screen.
- Send questions via the chat function.
- Conflicts of interest – If a Governor declares a conflict of interest, they will withdraw from the meeting by leaving the call. Once the Governing Body is ready for the Governor to re-join the meeting, the Clerk will notify them by email.
- If you have to leave the meeting early (as pre-arranged or for an unforeseen situation that arises during the meeting) communicate this via the chat function.
- If there is a technical difficulty which means that you cannot contribute to the meeting, communicate with the chair of the meeting via email or some other appropriate messaging facility to inform them of your situation and decide upon a way forward.

## **APPENDIX 3**

### **Subject Access Request Procedure**

Within an Academy responding to a SAR request is the responsibility of the Academy, a SAR related to the function of the Central Trust will be responded to by the DPO.

A subject access request can be made verbally, in writing or email, via text or social media. It is important that the date of the request is documented as there is one calendar month to respond to the request.

A request may not be termed subject access request, the requestor may simply ask for information that is held on them. A request for personal information will not be delayed just because it has not been given the official term.

Upon receipt of a SAR this should be immediately reported to the Academy Data Protection lead.

Confirmation of the SAR can be requested in writing however the individual is not obliged to comply with this. If not received in writing it is recommended that the Data Protection Lead immediately contacts the requestor to discuss the data that they are interested in obtaining, particularly if there is a large amount of data held about the individual.

The Data Protection Lead should inform the DPO of the SAR. In cases of complicated SARs then DPO will offer advice and guidance.

The SAR should then be acknowledged in writing. Standard documents are available from the DPO.

This request should be logged on the SAR Log pro-forma on Sharepoint.

If the requestor is known to the Academy/Trust there is no need for the requestor to provide proof of identity. If not known, then proof of identity should be obtained and recorded.

Whilst waiting for proof of identity, or clarification on the data required the clock can be stopped and the timescale to respond amended to reflect the time it has taken to receive the proof of identity. In circumstances like this this should be confirmed in writing to the requestor with the new reset date by which the information will be provided.

SARs can be requested on behalf of someone else e.g. a solicitor on behalf of a client or from a parent/carer on behalf of a child.

Where a solicitor has requested information then a signed consent form is required. If this is not provided then the clock can be stopped whilst waiting for this, and the procedure outlined above followed.

When a parent/carer makes a request the age and maturity of the child needs to be considered. If over 12 years and the child is able to understand their Data Protection rights then they could be asked to complete a consent form authorising the release of the information to parents/carers. An example form is available from the DPO.

If you feel the child is not able to understand or you have concerns about the consequences of releasing information to the child then the request must be discussed with the DPO who will advise

on the best course of action. The best interests of the child are at the centre of any requests for personal data.

Once the information has been collated, it should be reviewed and redacted for any information that doesn't relate to the individual.

There may be some information or circumstances where issuing the data can be withheld via exemptions under UK GDPR, please seek advice from the DPO.

A letter should accompany the issuance of the SAR, this will detail the date of issue, the date by which the SAR was due to be issued, details of the information that has been released and any exemptions. It should also detail the right to complain to the DPO in the first instance and the details of how to do this if they feel that the SAR has not been handled appropriately. An example letter is available on Sharepoint.

When releasing the SAR, consideration must be given to the safe transfer for this data. The requestor should be asked how they would like to receive the information.

If the Requestor is collecting this then they should do in person and sign to say they have received the information, if the information is released electronically it should be password protected and sent via encrypted email, if sent via hard copy then it should be posted via special delivery/courier (where the recipient has to sign for the information).

In instances where there have been repetitive requests for information, where they are deemed malicious or requesting further copies of information already provided, then please contact the DPO for guidance as this may be deemed as manifestly unfounded or excessive. The DPO will provide advice on an appropriate response.

## Appendix 4

### Data Protection Complaints Form

Please complete and return to the DPO [DPO@primitas.co.uk](mailto:DPO@primitas.co.uk). Receipt will be acknowledged within 30 working days

|                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Your name:                                                                                                                                                                 |
| Your address:<br><br><br><br><br><br><br><br><br><br>Postcode:<br><br>Email address:<br><br>Daytime contact number:<br><br>Evening contact number:                         |
| Your relationship to the Academy or Trust (e.g. student, parent, staff)                                                                                                    |
| Academy name or Central Trust:                                                                                                                                             |
| Detail of the complaint (e.g. what data use are you complaining about, specifically what data,<br><br><br><br><br><br><br><br><br><br>                                     |
| What action, if any, have you already taken to try and resolve the complaint?<br>(Who did you speak to and what was the response)?<br><br><br><br><br><br><br><br><br><br> |
| What actions do you feel might resolve the problem?<br><br><br><br><br><br><br><br><br><br>                                                                                |

Are you attaching any supporting material if so what is this?

Name

Signature