Information Governance & Data Protection Policy

Date Published	**June 2016**
Version	**5**
Last Approved Date	**February 2024**
Review Cycle	**Annual**
Review Date	**February 2025**

"Learning together, to be the best we can be"

1. Policy statement

1.1. Information and personal data are major assets that Nexus Multi Academy Trust has a responsibility and requirement to protect, and, where required by law, to publish. The aim of this policy can be described as:

1.1.1. To provide a framework for the management of information requests made to Nexus MAT, and the management and protection of personal data held by Nexus MAT;

1.1.2. To assist staff to meet the presumption in favour of disclosure of information, as required by legislation, to promote greater openness, provide increased transparency of decision making and build public trust and confidence;

1.1.3. To ensure all legal obligations on Nexus MAT are met in relation to data protection and information governance.

1.2. Our Trust aims to ensure that all personal data collected about staff, pupils, parents and carers, governors, visitors and other individuals is collected, stored and processed in accordance with UK data protection law.

2. Legislation and guidance

2.1. This policy meets the requirements of the:

2.1.1. UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020.

2.1.2. Data Protection Act 2018 (DPA 2018).

2.2. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the government on Generative artificial intelligence in education.

2.3. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's guidance for the use of surveillance cameras and personal information.

2.4. In addition, this policy complies with regulation 5 of the Education (Pupil Information) (England) Regulations 2005 and our funding agreement and articles of association.

3. Definitions

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

TERM	DEFINITION
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

4. The data controller

4.1. The Trust processes personal data relating to parents and carers, pupils, staff, governors, visitors and others, and therefore is a data controller. The Trust is registered with the ICO / has paid its data protection fee to the ICO.

5. Roles and responsibilities

Trustees

5.1. The trust board has overall responsibility for ensuring that our schools and staff comply with all relevant data protection obligations.

5.2. The **data protection officer** (DPO) is responsible for overseeing the implementation of this policy, monitoring compliance with data protection law, and developing related policies and guidelines where applicable. The DPO reports activities directly to the Trust Board and, where relevant, their advice and recommendations on school data protection issues. The DPO is also the first point of contact for individuals whose data the Trust processes, and for the ICO.

5.3. Our DPO is the Chief Executive Officer and is contactable via info@nexusmat.org

5.4. The Headteacher acts as the data controller on a day-to-day basis. All Headteachers will:

5.4.1. Implement this policy within their school;
5.4.2. Ensure compliance to it by their staff;
5.4.3. Additionally they will specifically ensure that:
5.4.3.1. All current and future users of Trust information are instructed in their data protection responsibilities and have access to and have read information governance policies and guidance;
5.4.3.2. Authorised users of computer systems/media are trained in their use and comply with policy and procedural controls to protect personal data;

5.4.3.3. Determine which individuals are given authority to access specific information systems. The level of access to specific systems which contain personal data should be on a job function need, irrespective of status;

5.4.3.4. Any breach of this policy, real or suspected, is reported to their line manager and/or DPO.

5.5. Staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the Trust of any changes to their personal data, such as a change of address
- Contacting the DPO, or specified delegate, 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
- Immediately 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

6.1. The UK GDPR is based on data protection principles that our Trust must comply with. The principles say that personal data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed
- Accurate and, where necessary, kept up to date

- Kept for no longer than is necessary for the purposes for which it is processed
- Processed in a way that ensures it is appropriately secure

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

7. Collecting personal data

7.1. We will only process personal data where we have 1 of 6 'lawful bases' (legal reasons) to do so under data protection law:

- The data needs to be processed so that the Trust can fulfil a contract with the individual, or the individual has asked the Trust to take specific steps before entering into a contract
- The data needs to be processed so that the Trust can comply with a legal obligation
- The data needs to be processed to ensure the vital interests of the individual or another person i.e. to protect someone's life
- The data needs to be processed so that the Trust, as a public authority, can perform a task in the public interest or exercise its official authority
- The data needs to be processed for the legitimate interests of the Trust (where the processing is not for any tasks the Trust performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden
- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent

7.2. For special categories of personal data, we will also meet 1 of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims

- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

7.3. For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise or defence of legal rights
- The data needs to be processed for reasons of substantial public interest as defined in legislation

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

7.5. We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect, or use personal data in ways which have unjustified adverse effects on them.

7.6. 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.

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

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

7.9. We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

7.10. In addition, 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 Trust's record retention schedule.

8. Sharing personal data

8.1. We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil 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 pupils – for example, IT companies. When doing this, we will:
    - Only appoint suppliers or contractors that can provide sufficient guarantees that they comply with UK data protection law
    - Establish a contract with the supplier or contractor 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

8.2. We will also share personal data with law enforcement and government bodies where we are legally required to do so.

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

8.4. Where we transfer personal data internationally, we will do so in accordance with UK data protection law.

9. Freedom of Information

9.1. Nexus Multi Academy Trust is committed to an access to information framework that ensures:

- All requests for information are dealt with promptly and within statutory timescales;
- Advice and assistance is offered to help any enquirer frame their request so that they receive the information they require;
- Requests are assessed to ensure the confidentiality of personal or commercially sensitive data is not breached;
- Information is withheld if a legitimate exemption applies and the application of the exemption is explained to the enquirer;
- All enquirers are kept informed in a timely manner of the progress of their request and of any delays to which it may be subject;
- Assistance is offered to any enquirer to help them understand the information they receive;
- All enquirers are advised of their rights to question the information received and know what has not been provided and why;
- All enquirers are advised of their right to take any appeal or complaint to an internal review process (where appropriate) or to the Information Commissioner, if they are dissatisfied with the service received or the information provided;
- All requests are monitored and performance reported to the Trust Board to ensure compliance with the legislation;
- All staff are provided with suitable training, guidance and procedures to enable them to manage requests for information;

9.2. The DPO is responsible for ensuring the access to information process is regularly audited to ensure compliance with statutory requirements, and that relevant national codes of practice are followed.

9.3. The DPO is responsible for ensuring the access to information process is regularly audited to ensure compliance with statutory requirements, and that relevant national codes of practice are followed.

9.4. All Requests for information should be made via the online form on the Nexus Multi Academy Trust website, Contact | Nexus Multi Academy Trust (nexusmat.org).

9.5. The Trust will make the information available to the requestor within the statutory 20 working days unless a Public Interest Test (PIT) is necessary. If a PIT is necessary, the requestor will be notified that the time limit will be extended by another 20 days.

9.6. If the Trust considers that an exemption applies in accordance with legislation and ICO guidance and does not consider that disclosure is appropriate, the requester must also be informed of this within 20 working days of making the request.

9.7. If an exemption is considered to apply, the decision not to disclose information should be made by the academy, in consultation with the Data Protection Officer, and the reasons for non-disclosure documented.

9.8. Requests will be authorised by the relevant Headteacher, after consultation with the DPO, before release to the requester.

9.9. The Trust Board will be informed of any request relating to their duties by the Chief Executive Officer.

9.10. Before applying section 14 and deeming a request **vexatious** under the Freedom of Information Act 2000, the Headteacher will consult the Data Protection Officer for their advice. The advice of the DPO should always be followed. In circumstances where the Headteacher and DPO disagree, the matter should be referred to the Chief Executive Officer in writing.

10. Subject access requests and other rights of individuals

Subject access requests

10.1. Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing
- The right to lodge a complaint with the ICO or another supervisory authority
- 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
- The safeguards provided if the data is being transferred internationally

10.2. Subject access requests can be submitted in any form, but we may be able to respond to requests more quickly if they are made in writing and include:

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

10.3. If staff receive a subject access request in any form they must immediately forward it to the DPO.

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

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

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

10.7. 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 (or receipt of the additional information needed to confirm identity, where relevant)
- 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

10.8. We may not disclose information for a variety of reasons, such as if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is being or has been abused, or is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts

10.9. If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

10.10. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

10.11. 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 (in certain circumstances)
- Prevent use of their personal data for direct marketing

- Object to processing that has been justified on the basis of public interest, official authority or legitimate interests
- Challenge decisions based solely on automated decision making or profiling (i.e. making decisions or evaluating certain things about an individual based on their personal data with no human involvement)
- 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)

10.12. 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.

10.13. The rights of data subjects are subject to **certain statutory exemptions**. Nexus Multi Academy Trust will disclose personal information, without the data subject's consent in accordance with the General Data Protection Regulation (2018).

11. Parental requests to see the educational record

11.1. Parents, or those with parental responsibility, have a right to access their child's educational record (which includes most information about a pupil) we will usually aim to provide this within 15 school days of receipt of a written request – to foi@nexusmat.org.

11.2. We may charge a fee to cover the cost of supplying the record if necessary and would always outline this to the requester before processing, any fee would only be to recover the administration and supply costs.

11.3. There are certain circumstances in which a record would not be released, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

12. CCTV

12.1. We use CCTV in various locations around school sites to ensure they remain safe. We will follow the ICO's guidance for the use of CCTV, and comply with data protection principles.

12.2. 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.

12.3. Any enquiries about the CCTV system should be directed to the Trust via info@nexusmat.org

13. Photographs and videos

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

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

13.3. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

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

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

13.6. Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social

media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

13.7. Where a school takes photographs and videos, 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 a school website or social media pages

13.8. 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.

13.9. 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.

14. Artificial intelligence (AI)

14.1. Artificial intelligence (AI) tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard. We recognise that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

14.2. 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.

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

15. Data protection by design and default

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

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge

- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6)
- Completing data protection impact assessments where the Trust'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 position and contact details of our Trust 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

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

16.2. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, or left anywhere else where there is general access

- Where personal information needs to be taken off site, staff must sign it in and out from the school/Trust office
- Passwords that are at least 10 characters long containing letters and numbers are used to access Trust computers, laptops and other electronic devices. Staff and pupils are reminded that they should not reuse passwords from other sites
- Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for Trust-owned equipment (see our policy on acceptable use)
- 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)

17. Disposal of records

17.1. 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.

17.2. 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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

17.3. Our retention schedule lists how long we retain certain information and how it is disposed.

18. Personal data breaches

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

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

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

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

19. Training

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

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

20. Monitoring arrangements

20.1. The DPO is responsible for monitoring and reviewing this policy.

20.2. This policy will be reviewed and approved annually by the Trust board.

Appendix 1: Personal data breach procedure

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

On finding or causing a breach or potential breach, the staff member, governor or data processor must immediately notify the data protection officer (DPO) by completing the Trust provided form.

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

Staff and governors will co-operate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the relevant headteacher or executive leader.

The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).

The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.

The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored centrally.

Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the Trust's awareness of the breach. 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 of the Trust's awareness of the breach. 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.

Where the Trust is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:

- A description, in clear and plain language, of the nature of the personal data breach
- 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 consider, in light of the investigation and any engagement with affected individuals, whether to 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 centrally.

The DPO and headteacher (or executive leader in the central team) will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible.

The DPO and headteacher (or executive leader in the central team) will meet regularly to assess recorded data breaches and identify any trends or patterns requiring action by the Trust to reduce risks of future breaches.

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, 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.

i. Sensitive information being disclosed via email (including safeguarding records)

If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error.

Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error.

If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the ICT department to attempt to recall it from external recipients and remove it from the Trust's email system (retaining a copy if required as evidence).

In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to 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.

- We will endeavour to obtain a written response from all the individuals who received the data, confirming that they have complied with this request.
- We 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.

- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the Trust should inform any, or all, of its local safeguarding partners.

ii. Hardcopy reports sent to the wrong pupils or families.

If physical copies of sensitive data are misplaced, the incident must be reported immediately. Every effort must be made to retrieve the physical document from the recipient, or, at the very least, request them to securely destroy the document.

Staff must ensure that physical documents, such as those sent via post or fax, are transferred to the intended recipient with care.

If a staff member repeatedly sends physical copies of data, disciplinary action may be taken.

Appendix 2: Appropriate Policy Document

As part of Nexus Multi Academy Trust's statutory and corporate functions, we process special category data and criminal offence data in accordance with the requirements of Article 9 and 10 of the General Data Protection Regulation ('UK GDPR') and Schedule 1 of the Data Protection Act 2018 ('DPA 2018').

i. Special Category Data

Special category data is defined at Article 9 of the UK GDPR as personal data revealing:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- 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.

ii. Criminal Offence Data

Article 10 of the UK GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

iii. The Policy Document

Some of the Schedule 1 conditions for processing special category and criminal offence data require us to have an Appropriate Policy Document ('APD') in place, setting out and explaining our procedures for securing compliance with the principles in Article 5 and policies regarding the retention and erasure of such personal data.

This document explains our processing and satisfies the requirements of Schedule 1, Part 4 of the DPA 2018.

In addition, it provides some further information about our processing of special category and criminal offence data where a policy document isn't a specific requirement.

The information supplements our privacy notice.

Our processing of special category and criminal offence data for law enforcement purposes is not covered in this document. Processing for law enforcement purposes is carried out by us in our capacity as a competent authority and falls under Part 3 of the DPA 2018.

iv. Conditions for Processing Special Category and Criminal Offence Data

We process special categories of personal data under the following of the UK GDPR Articles:

Article 9(2)(b) – where processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on Nexus Multi Academy Trust or the data subject in connection with employment, social security or social protection.

Examples of our processing include staff sickness absences and conflicts of interest.

Article 9(2)(g) - reasons of substantial public interest.

Our processing of personal data in this context is for the purposes of substantial public interest and is necessary for the carrying out of our role.

Examples of our processing include the information we seek or receive as part of investigating a complaint.

Article 9(2)(f) – for the establishment, exercise or defence of legal claims.

Examples of our processing include processing relating to any employment tribunal or other litigation.

Article 9(2)(a) – explicit consent

In circumstances where we seek consent, we make sure that the consent is unambiguous and for one or more specified purposes, is given by an affirmative action and is recorded as the condition for processing.

Examples of our processing include staff dietary requirements and health information we receive from our customers who require a reasonable adjustment to access our services.

Article 9(2)(c) – where processing is necessary to protect the vital interests of the data subject or of another natural person.

An example of our processing would be using health information about a member of staff in a medical emergency.

We process criminal offence data under Article 10 of the UK GDPR.

Examples of our processing of criminal offence data include pre-employment checks and declarations by an employee in line with contractual obligations.

v. Processing which requires an Appropriate Policy Document

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD.

This section of the policy is the APD for Nexus Multi Academy Trust. It demonstrates that the processing of special category ('SC') and criminal offence ('CO') data based on these specific Schedule 1 conditions is compliant with the requirements of the UK GDPR Article 5 principles. In particular, it outlines our retention policies with respect to this data.

Description of data processed

We process the special category data about our employees that is necessary to fulfil our obligations as an employer. This includes information about their health and wellbeing, ethnicity, photographs and their membership of any trade union.

Our processing for reasons of substantial public interest relates to the data we receive or obtain in order to fulfil our statutory functions.

We also maintain a record of our processing activities in accordance with Article 30 of the UK GDPR.

Further information about this processing can be found in our privacy notice.

vi. Accountability Principle

We have put in place appropriate technical and organisational measures to meet the requirements of accountability. These include:

- The appointment of a data protection officer
- Taking a 'data protection by design and default' approach to our activities
- Maintaining documentation of our processing activities
- Adopting and implementing data protection policies and ensuring we have written contracts in place with our data processors
- Implementing appropriate security measures in relation to the personal data we process
- Carrying out data protection impact assessments for our high risk processing
- We regularly review our accountability measures and update or amend them when required.

Lawfulness, fairness and transparency

Processing personal data must be lawful, fair and transparent. It is only lawful if and to the extent it is based on law and either the data subject has given their consent for the processing, or the processing meets at least one of the conditions in Schedule 1.

We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and this policy document.

Our processing for the purposes of employment relates to our obligations as an employer.

Purpose limitation

We will not process personal data for purposes incompatible with the original purpose it was collected for.

Data minimisation

We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Accuracy

Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights don't apply, we will document our decision.

Storage limitation

All special category data processed by us for the purpose of employment, unless retained longer for archiving purposes. We determine the retention period for this data based on our legal obligations and the necessity of its retention for our business needs.

Integrity and confidentiality (security)

Electronic information is processed within our secure network. Hard copy information is processed in line with our security procedures.

Our electronic systems and physical storage have appropriate access controls applied.

The systems we use to process personal data allow us to erase or update personal data at any point in time where appropriate.

vii. Additional Special Category Processing

We process special category personal data in other instances where it is not a requirement to keep an appropriate policy document. Our processing of such data respects the rights and interests of the data subjects. We provide clear and transparent information about why we process personal data including our lawful basis for processing in our privacy notice and staff privacy notice.