Nexus Education Schools Trust

Data Protection Policy

Date: July 2024
Review Date: July 2026

Contents

1. Introduction

1.1 Nexus Education Schools Trust "(**the Trust"**) is committed to complying with its data protection obligations, and to being concise, clear and transparent about how it obtains and uses personal data relating to the Trust community, including pupils, parents and staff.

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

1.3 This policy sets out how we comply with our data protection obligations set out in the UK General Data Protection Regulation (the "UK GDPR") and the Data Protection Act ("DPA") 2018.

1.4 The aim of this policy is to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal data to which they may have access in the course of their duties.

1.5 The Trust has appointed a Data Protection Officer as the person with overall responsibility for data protection compliance (the Data Protection Officer ("DPO"). Any questions about this policy or requests for further information should be directed to them. The [DPL/DPO] may be contacted via office@nestschools.org

2. Scope

2.1 This policy applies to all staff at the Trust, including its schools. Any reference to the term 'staff' in this policy includes employees, local committee members, trustees, volunteers, consultants, contractors, trainees, temporary workers, visiting music teachers (VMTs), any peripatetic workers and sports coaches, agency workers and casual workers.

2.2 Staff should refer to the Trust's other relevant policies including those relating to information security, data retention, bring your own device (BYOD), and personal data breaches, which contain further information regarding the protection of personal data in those contexts.

2.3 We will review and update this policy bi-annual in accordance with our data protection obligations. We will circulate any new or materially modified policy to staff when it is adopted.

All staff are required to read and confirm that they understand this policy. Please confirm this by completion of an online form and the link will be forwarded to you by your Headteacher.

3. Legislation and guidance

This policy meets the requirements of the UK GDPR and the DPA 2018.

It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and guidance from the Department for Education (DfE) on Generative artificial intelligence in education.
It also reflects the ICO's guidance for the use of surveillance cameras and personal information. In addition, this policy complies with our funding agreement and articles of association.

4. 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.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

5. The data controller

The Trust processes personal data relating to parents and carers, pupils, staff, local committee members, visitors and others, and is the data controller of that personal data.

The Trust is registered as a data controller with the ICO and will renew this registration annually, as legally required.

6. Roles and responsibilities

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

6.1 Local Committee

The governing board has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

6.2 Data protection officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.

They will provide an annual report of their activities directly to the governing board and, where relevant, report to the board their advice and recommendations on school data protection issues.

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

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

The DPO is based at NEST Central Team and can be contacted at office@nestschools.org

6.3 Headteacher

Headteachers have overall responsibility for implementing guidance from the Trust and/or the DPO on a day-to-day basis.

6.4 All staff

All staff are responsible for:

- Collecting, storing and processing any personal data in accordance with this policy
- 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 or a suspected 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

7. Data protection principles

7.1 When processing personal data, the Trust and its staff must comply with the data protection principles set out in Article 5 of the UK GDPR as follows:

7.1.1 we will process personal data lawfully, fairly and in a transparent manner ('***lawfulness, fairness and transparency***');

7.1.2 we will collect personal data for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes ('***purpose limitation***');

7.1.3 we will only process the personal data that is adequate, relevant and necessary for the relevant purposes ('***data minimisation***');

7.1.4 we will keep accurate and up to date personal data, and take reasonable steps to ensure that inaccurate personal data is deleted or corrected without delay ('***accuracy***');

7.1.5 we will keep personal data in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data is processed ('***storage limitation***'); and

7.1.6 we will take appropriate technical and organisational measures to ensure that personal data is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage ('***integrity and confidentiality***').

7.2 In addition, the Trust is also responsible for, and must be able to demonstrate compliance with, the above principles ('***accountability***'). This means that we will:

7.2.1 inform individuals about how and why we process their personal data, usually by way of a privacy notice;
7.2.2 be responsible for checking the quality and accuracy of the data;
7.2.3 regularly review the records held to ensure that data is not held longer than is necessary, and that it has been held in accordance with our records retention policy;
7.2.4 ensure that when data is authorised for disposal it is disposed of / deleted appropriately;
7.2.5 ensure appropriate security measures to safeguard personal data whether it is held in paper files or electronically, and follow the requirements set out in our information security policy at all times;
7.2.6 share personal data with others only when it is necessary and legally appropriate to do so;
7.2.7 set out clear procedures for responding to requests for access to personal data known as subject access requests and other rights exercised by individuals in accordance with the UK GDPR); and
7.2.8 report any actual or suspected personal data breaches in accordance with this policy.

8. Lawfulness, fairness and transparency

8.1 The Trust is responsible for ensuring that personal data is processed in a lawful, fair and transparent way. In relation to any processing activity we will undertake the actions below before the processing begins, and then regularly while it continues:

8.1.1 review the purposes of the particular processing activity, and identify which of the following legal bases for processing (as set out in Article 6 of the UK GDPR) is most appropriate:

- 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 or another person i.e. 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 or exercise its official authority**
- The data needs to be processed for the **legitimate interests** of the school (where the processing is not for any tasks the school 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**

8.1.2 Except where the processing is based on consent, we will satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
8.1.3 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);
8.1.4 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

8.1.5 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 DPA 2018.

8.2 When determining whether the legal basis of legitimate interests is appropriate, we will:

8.2.1 carry out a legitimate interests assessment ("LIA") and keep a record of it, to ensure that we can justify our decision;
8.2.2 if the LIA identifies a significant risk to an individual's data protection rights, consider whether we also need to conduct a data protection impact assessment ("DPIA");
8.2.3 keep the LIA under review, and repeat it if circumstances change; and
8.2.4 include information about our legitimate interests in our relevant privacy notice(s).

8.3 Where processing of personal data is likely to result in a high risk to individuals, we will, before commencing the processing, carry out a DPIA to assess:

8.3.1 whether the processing is necessary and proportionate in relation to its purpose;
8.3.2 the risks to individuals; and
8.3.3 what measures can be put in place to address those risks and protect personal data.

8.4 In order to comply with its transparency obligations, the Trust will issue privacy notices from time to time, informing data subjects about the personal data that we collect and hold, how they can expect personal data to be used and for what purposes. We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

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.

9. Purpose Limitation

9.1 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.
9.2 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.

10. Data Minimisation

10.1 The Trust will ensure that the processing of personal data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

10.2 You may only collect personal data to the extent required for your duties, and should ensure that any personal data collected is adequate and relevant for the intended purposes. In order to do this, you should:

10.2.1 minimise the processing of personal data, for example, through redaction and the deletion of long emails trails, by minimising access to, and sharing of, personal data to include only that which is necessary;
10.2.2 anonymise personal data where appropriate;
10.2.3 pseudonymise personal data where possible, for example, through the use of initials rather than full names; and
10.2.4 ensure that when personal data is no longer needed, it is deleted in accordance with the Records Retention and Deletion Policy.

11. Accuracy

11.1 Personal data must be accurate and kept up to date. It must be corrected or deleted without delay when it is inaccurate.

12. Storage Limitation

12.1 Personal data should not be kept for any longer than is necessary for the purposes for which the personal data is processed.
12.2 The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal data was obtained. Staff should follow guidance contained in our Records Management Policy/Data Retention Schedule, which sets out the relevant retention period, or the criteria that should be used to determine the retention period.
12.3 Personal data that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

13. Integrity and Confidentiality

13.1 The Trust will use appropriate technical and organisational measures in accordance with our information security policy to keep personal data secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
13.2 Before any new agreement involving the processing of personal data by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the [DPO].
13.3 All staff have an obligation to report actual or suspected personal data breaches to the [DPO] immediately upon discovery.

14. Documentation and Records

14.1 We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve special category data or criminal offence data, including:

14.1.1 the purposes of the processing;
14.1.2 a description of the categories of individuals and categories of personal data;
14.1.3 categories of recipients of personal data;
14.1.4 where relevant, details of transfers of personal data outside the UK, including documentation of the transfer mechanism safeguards in place;
14.1.5 where possible, retention schedules; and
14.1.6 where possible, a description of technical and organisational security measures.

14.2 As part of our record of processing activities we document, or link to documentation, on:

14.2.1 information required for privacy notices;
14.2.2 records of consent;
14.2.3 controller-processor contracts;
14.2.4 the location of personal data;
14.2.5 DPIAs; and
14.2.6 records of personal data breaches.

14.3 If we process special category data or criminal offence data, we will keep written records of:

14.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
14.3.2 the lawful basis and additional conditions relied upon to process this data; and
14.3.3 whether we retain and erase the personal data in accordance with our Records Management Policy/Data Retention Schedule and, if not, the reasons for not following it.

14.4 We will conduct regular reviews of the personal data we process and update our documentation accordingly.

15. Individual obligations

15.1 You may have access to the personal data of others including members of staff, pupils, parents, teachers and other third parties who may come into contact with the Trust or its schools in the course of your employment or engagement. If so, the Trust expects you to help meet its data protection obligations to those individuals.
15.2 If you have access to personal data, you must:

15.2.1 only access the personal data that you have authority to access, and only for authorised purposes;
15.2.2 only allow other staff to access personal data if they have appropriate authorisation;
15.2.3 only allow individuals who are not staff to access personal data if you have specific authority to do so from the [DPO];
15.2.4 keep personal data; and
15.2.5 to the extent that you may use personal devices for work purposes, comply with the Trust's BYOD Policy.

16. Working remotely

16.1 As part of our commitment to flexible working, the Trust supports homeworking in appropriate circumstances, either occasionally (to respond to specific circumstances or to complete particular tasks) and in some cases on a regular basis (full or part-time).
16.2 Working remotely can lead to increased risk in terms of the security of Trust information (including personal data) and communications systems. When working remotely, you must comply with all relevant policies, including our:

16.2.1 Staff Data Protection Policy (this policy);
16.2.2 Information Security Policy;
16.2.3 Bring Your Own Device (BYOD) policy;
16.2.4 Records Management Policy/Data Retention Schedule; [and]

17. Rights of individuals

Data subjects have various rights in relation to their personal data. Depending on the circumstances, data subjects have the right:

- to be informed about how, why and on what basis that data is processed (the Trust usually provides this information to data subjects via its Privacy Notice(s));

- to obtain confirmation that data is being processed and to obtain access to it and certain other information by making a subject access request;
- to have personal data corrected if it is inaccurate or incomplete (known as the right of rectification);
- to have personal data erased in certain circumstances (sometimes known as the right to be forgotten);
- to restrict the processing of personal their personal data in certain circumstances (e.g., if there is a complaint about accuracy);
- to object to the processing of their personal data in certain circumstances;
- to ***receive*** personal data that they have provided in a structured, commonly used and machine-readable format and to request that their personal data is ***transferred*** to another organisation (known as the right to data portability)

18. The right to access - subject access requests

Individuals have a right to make a 'Subject Access Request' to gain access to personal information that the Trust or its schools holds about them together with other information about how their data is used (known as supplementary information). This legal right is called the right of access, often referred to as a Subject Access Request or SAR. There are some legal exemptions that mean that requesters may not always be entitled to a copy of all of their personal data that we hold.

18.1 As part of a subject access request, data subjects are entitled to the following:

- 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

18.2 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

18.3 If you, as a member of staff, receive a SAR from a pupil, parent or carer or other person, you should immediately inform the DPO. The DPO, has a legal duty to deal with SARs without delay and at the latest within one month of receipt (subject to the rights of Trust to extend the time limit for response by a further two months, considering the complexity and number of the requests, in accordance with Article 12(3) of the UK GDPR).

18.4 Any individual, including a child or young person, may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the request and the DPO must be confident of the identity of the individual making the request.

18.5 Where a child or young person lacks the capacity to understand their rights and the implications of making a Subject Access Request (e.g., due to their age or some other reason) a third party, such as a parent or carer, can make a request on their behalf. The DPO must, however, be satisfied that:

18.5.1 the child or young person lacks sufficient understanding of their own data rights; **and**

18.5.2 the request made on behalf of the child or young person is made in the child or young person's best interests.

18.6 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.

18.7 When responding to Subject Access 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

18.8 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.

18.9 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.

18.10 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.

18.11 All files must be reviewed and applicable exemptions under the UK GDPR and the DPA must be applied by the DPO. Any disclosure can only take place after the response is approved by the DPO. Any response sent to the requestor must comply with the requirements of the UK GDPR and must include the supplementary information the requestor is entitled to.

18.12 Where some of the data in a document cannot be disclosed a copy of the full document and the altered document should be retained, with the reason why the document was altered.

19. Right to rectification

19.1 Data subjects have the right to request the rectification of inaccurate or incomplete data verbally or in writing. Any request for rectification should be sent to the DPO immediately.

19.2 Where personal data is identified as inaccurate or incomplete, it shall be amended, and the data subject notified of the same without undue delay and in any event within one month (unless this deadline is extended in accordance with the UK GDPR).

19.3 Where a request is refused, the request and reasons for refusal shall be documented and notice of refusal should be provided to the individual within a month of receipt of the request. The Trust will include in its response the reasons why the request has been refused and information about the individual's right to complain to the ICO and to bring a civil claim.

20. Right to erasure

20.1 Individuals have a right, in certain circumstances, to have their personal data permanently erased. Individuals may exercise this right in writing or verbally.

20.2 The right to erasure is also known as the 'right to be forgotten' and arises in the following circumstances:

20.2.1 where the personal data is no longer necessary for the purpose or purposes for which it was collected and processed;
20.2.2 where consent is the legal basis for processing and that consent is withdrawn;
20.2.3 where legitimate interests is the legal basis for processing and the individual objects to the processing of their data, and there is no overriding legitimate interest to continue processing;
20.2.4 where the Trust is processing the personal data for direct marketing purposes and the individual objects to that processing;
20.2.5 where personal data is being unlawfully processed;
20.2.6 where there is a legal obligation on the Trust to delete the personal data; or
20.2.7 where the Trust has processed the personal data to offer information society services to a child.

20.3 Any request for erasure should be sent to the DPO immediately. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).

20.4 The DPO will determine the outcome of any request for erasure of personal data. Where a decision is made to erase the data, and this data has been passed to other controllers, and / or has been made public, the Trust will inform those organisations of the request unless this proves impossible or involves disproportionate effort.

20.5 Where a request is refused, the Trust will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

21. Right to restrict processing

21.1 In the following circumstances, individuals have the right to request the restriction or suppression of their personal data in writing or verbally:

21.1.1 where the accuracy of personal data has been contested, during the period when the Trust is attempting to verify the accuracy of the data;
21.1.2 where processing has been found to be unlawful, and the individual has asked that there be a restriction on processing rather than erasure;
21.1.3 where personal data would normally be deleted, but the individual has requested that their personal data be kept for the purpose of the establishment, exercise or defence of a legal claim;
21.1.4 where there has been an objection to the processing, pending the outcome of any decision.

21.2 Any request for restriction should be sent to the DPO immediately. The request must be complied with within one calendar month (unless this deadline is extended in accordance with the UK GDPR).
21.3 The DPO will determine the outcome of any request for restriction of processing personal data. As matter of good practice, the Trust will automatically restrict the processing whilst considering the accuracy or legitimate grounds for processing the personal data in question.
21.4 Where processing has been restricted, such personal data shall (with the exception of storage) be processed only in the following circumstances:

21.4.1 with the consent of the data subject;
21.4.2 where processing is necessary for the establishment, exercise or defence of legal claims;
21.4.3 for the protection of rights of another person (including a company); or
21.4.4 for reasons of important public interest.

21.5 If the Trust has disclosed the personal data in question to others, it will contact each recipient to inform them of the restriction, unless this proves impossible or involves disproportionate effort.
21.6 Once the Trust has determined the accuracy of the data, or whether its legitimate grounds override those of the data subject, the Trust may decide to lift the restriction. The Trust will inform the requestor before the restriction is lifted.

21.7 Where a request is refused, the Trust will inform the individual without undue delay and within one month of receipt of the request. The response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

22. Right to object

22.1 Where personal data is being processed for direct marketing purposes, an individual has the right to object at any time to processing of their personal data for such purposes. This right is absolute and where such an objection is made the Trust will stop processing personal data for this purpose.

22.2 An individual also has the right to object to the processing of their personal data on the legal basis of:

22.2.1 a task carried out in the public interest;
22.2.2 the exercise of official authority vested in the Trust; or
22.2.3 the legitimate interests of the Trust or a third party.

22.3 Where such an objection is made, it must be sent to the DPO immediately. The DPO will assess whether the processing should cease or whether there are compelling legitimate grounds to continue processing which override the interests, rights and freedoms of the individuals concerned, or whether the data is required for the establishment, exercise or defence of legal proceedings.

22.4 The DPO is responsible for notifying the individual of the outcome of their assessment without undue delay and within one calendar month of receipt of the objection (unless this deadline is extended in accordance with the UK GDPR). If the request is refused, the response will include the reasons for the refusal and information about the individual's right to complain to the ICO and to bring a civil claim.

23. Right to data portability

23.1 Individuals have the right to receive their personal data in a structured, commonly used, and machine-readable format, and to require the Trust to transmit that personal data directly to another controller in certain circumstances.

23.2 This right only applies to data provided to the Trust directly by the data subject and:

23.2.1 The processing is on the basis of consent or to perform a contract; and
23.2.2 the processing is carried out by automated means (i.e. on a computer).

23.3 If such a request for this is made, it should be forwarded to the DPO immediately and this will be reviewed and actioned as necessary.

24. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will follow the ICO's guidance for the use of CCTV and comply with data protection principles.

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 should be directed to the DPO.

25. Photographs and videos

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

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.

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.

Where the 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 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 Child Protection and Safeguarding Policy at www.nestschools.org for more information on our use of photographs and videos.

26. Artificial intelligence (AI)

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.

Nexus Education Schools Trust recognises that AI has many uses to help pupils learn, but also poses risks to sensitive and personal data.

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.

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

27. Data protection 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
- 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 school 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

28. 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 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 office
- Passwords that are at least 10 characters long containing letters and numbers are used to access school 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 local committee members who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment (see our online safety policy/acceptable use agreements 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

29. 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.

30. Personal data breaches

In the unlikely event of an actual or suspected data breach, all staff must follow the procedure set out in appendix 1.

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

31. Training

The Trust will ensure that staff are adequately trained regarding their data protection responsibilities.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

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

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

32. Consequences of failing to comply

32.1 The Trust takes compliance with this policy very seriously. Failure to comply with the policy:

32.1.1 puts at risk the individuals whose personal data is being processed;
32.1.2 carries the risk of significant sanctions for the individual and the Trust;
32.1.3 may, in some circumstances, amount to a criminal offence by the individual.

32.2 Because of the importance of this policy any failure to comply with any requirement of it may lead to disciplinary action, which may result in termination of your relationship with the Trust.

33. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy.

This policy will be reviewed every 2 years and shared with the local committees and NEST trustees.

34. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme
- Child Protection & Safeguarding policy
- Privacy Notice for Parents/Carers
- Privacy Notice for Staff
- Acceptable Use Policy
- Online Safety Policy

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 a suspected breach, the staff member, local committee member or data processor must immediately notify the data protection officer (DPO) by completing the data breach form which is available at www.nestschools.org
- 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 local committee members 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 headteacher and the chair of the local committee.
- The Trust 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 Trust should take external advice when required (e.g. from IT providers or legal advice). (See the actions relevant to specific data types 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) 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 by NEST.
- 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 school'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 school'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 school 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 will be stored centrally at NEST.
- The DPO and headteacher will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible

Actions to minimise the impact of data breaches

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.

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/external IT support provider] to attempt to recall it from external recipients and remove it from the school'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
- The DPO will endeavor to obtain 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
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.

Other types of breach that you might want to consider could include:

- Details of pupil premium interventions for named children being published on the school website
- Non-anonymised pupil 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
- Hardcopy reports sent to the wrong pupils or families.