Nishkam School Trust

Data Protection Policy

Approved by:	Trustees	**Date:** 23 February 2021
Last reviewed on:	January 2021	
Next review due:	January 2023	

Contents

Our Vision and Ethos

Nishkam schools are Sikh ethos multi faith schools that take a distinctive approach to many traditional faith schools. The Nishkam School Trust education model is led by virtues such as, compassion, humility, service, contentment, optimism, trust and forgiveness. Virtues are prevalent throughout our teaching and learning model and are modelled by our pupils, staff and teachers. Our pupils explore the divine context of humanity and wonder of all creation and also learn from the wisdom of all religions and in doing so explore the infinite human potential to do good unconditionally. We support all pupils and staff to develop aspects of their own religious, spiritual or human identities. In service of God, we pray for guidance in this endeavour and forgiveness for the errors we may make.

1. Aims

Nishkam School Trust aims to ensure that all personal data collected about staff, pupils, parents, governors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (EU) 2016/679 (GDPR) and the Data Protection Act 2018 (DPA 2018). This policy applies to all school's within the Trust and all personal data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the GDPR and the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR. 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 code of practice for the use of surveillance cameras and personal information.

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

3. Definitions

Term	Definition
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 of 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.

4. The data controller

Our school processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.
The school is registered with the ICO and has paid its data protection fee to the ICO, as legally required.

5. Roles and responsibilities

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

5.1 Trust Board

The Trust Board has overall responsibility for ensuring that our school's comply with all relevant data protection obligations.

5.2 Data Protection Officer

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. The DPO is the first contact for the ICO (Information Commissioners Office). They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the Trust their advice and recommendations on school data protection issues. Our DPO is Rita Patel and is contactable via DPO@nishkamschools.org.

The DPL (Data Protection Lead) in each school is responsible for helping to comply with NST's obligations. All queries regarding data protection should be raised with the DPL in the first instance.

5.3 Principal/ Headteacher

The Principal/ Headteacher acts as the representative of the data controller on a day-to-day basis.

5.4 All staff

For the purpose of this guidance, all staff includes all paid and unpaid colleagues, volunteers, governors, trustees and members. All are responsible for;

- Collecting, storing and processing any personal data in accordance with this policy
- Informing the school of any changes to their personal data, such as a change of address

Contacting the DPO in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
- If they have any concerns that this policy is not being followed;
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area;
- If there has been a data breach;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals;

- If they need help with any contracts or sharing personal data with third parties.

6. Data protection principles

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

- Processed lawfully, fairly and in a transparent manner;
- Collected for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed;
- Accurate and, where necessary, kept up to date;
- Kept for no longer than is necessary for the purposes for which it is processed;
- Processed in a way that ensures it is appropriately secure;

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

7. Collecting personal data

7.1 Lawfulness, fairness and transparency

We will only process personal data where we have one of 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 school 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 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;**

For special categories of personal data, we will also meet one 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

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

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

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.

7.2 Limitation, minimisation and accuracy

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

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so, and seek consent where necessary. Staff must only process personal data where it is necessary in order to do their jobs.

We will keep data accurate and, where necessary, up-to-date. Inaccurate data will be rectified or erased when appropriate. 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 school's record retention schedule.

8. Sharing personal data

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 which can provide sufficient guarantees that they comply with 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

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

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

9. Subject access requests and other rights of individuals

9.1 Subject access requests

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

- Confirmation that their personal data is being processed;
- Access to a copy of the data;
- The purposes of the data processing;
- The categories of personal data concerned;
- Who the data has been, or will be, shared with;
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- 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.

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

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

9.2 Children and subject access requests

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

Children 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 at our school 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.

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 at our school 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.

9.3 Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request (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

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

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.

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.

9.4 Other data protection rights of the individual

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

- Withdraw their consent to processing at any time
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Object to processing which 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)

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

10. Parental requests to see the educational record

If the request is for a copy of the educational record, the school may charge a fee to cover the cost of supplying it. This right applies as long as the pupil concerned is aged under 18. There are certain circumstances in which this right can be denied, 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.

11. Biometric recognition systems

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

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

Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils. For example, pupils can pay for school dinners in cash at each transaction if they wish. Parents/carers and pupils can withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

As required by law, if a pupil refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the pupil's parent(s)/carer(s). Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

12. CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV. We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Principal/ Headteacher and Data Protection Officer.

13. 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 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.
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.

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

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.

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 for more information on our use of photographs and videos.

14. 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 (see section 6)
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Regularly training members of staff on data protection law, this policy, any related policies and any other data protection matters; we will also keep a record of attendance
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant
- Appropriate safeguards being put in place if we transfer any personal data outside of the European Economic Area (EEA), where different data protection laws will 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 EEA and the safeguards for those, retention periods and how we are keeping the data secure.

15. 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 governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment;
- 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

16. 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.

17. Personal data breaches

NST will make all reasonable endeavours to ensure that there are no personal data breaches. A personal data breach includes the loss of personal data; accidental or unlawful destruction of personal data; disclosure of personal data to an unauthorized third party; unlawful or accidental alternation of personal data or unauthorised access to personal data.

If in doubt of whether an incident constitutes a data breach they must refer the matter to the DPL or DPO immediately. In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix A.

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

18. Training

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 the school's processes make it necessary.

19. Monitoring arrangements

The DPO is responsible for monitoring and reviewing this policy. This policy will be reviewed every **2 years** and shared with the Trust Board.

20. Links with other policies

This data protection policy is linked to our:

- Freedom of information publication scheme;
- Online Safety Policy;
- Telecommunications and Computer Use Policy;
- CCTV Policy and Procedures;
- Privacy Notices;
- Policy photograph consent form;
- Safeguarding and Child Protection Policy

Appendix A: Data breach procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. Identification of breach

On finding or causing a breach, or potential breach, the staff member, trustee, governor or data processor must immediately notify the DPO. All breaches or potential breaches will be logged and stored centrally and held based on the retention schedule.

The DPO will undertake the following actions;

- Determine whether a breach has occurred and identify what personal data is at risk;
- Take immediate measures to prevent the breach from worsening with the support of key members of staff, for example changing passwords;
- Recover any compromised personal data, using back ups;
- Notify any outside agencies where required. For example notifying the police in a case that may lead to serious harm to a pupil/colleague;
- Consider whether the individuals affected be notified immediately so that they need to take action to protect their personal data

2. Assessing the risks

	Question	NST Response
1.	Precisely what data has been (or is thought to have been) lost, damaged or compromised?	
2.	Is any of the data Critical Personal Data as defined in this Data Protection Policy? • Information concerning child protection matters; • Information about serious or confidential medical conditions and information about special educational needs; • Information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved); • Financial information (for example about parents and staff); • Information about an individual's racial or ethnic origin; and • Political opinions; • Religious beliefs or other beliefs of a similar nature; • Trade union membership; • Physical or mental health or condition; • Genetic information; • Sexual life; • Information relating to actual or alleged criminal activity; and • Biometric information (e.g. A pupil's fingerprints following a criminal investigation).	
3	Who are the affected individuals e.g. staff, parents, pupils, trustees, governors, third parties?	
4	How many individuals have definitely been affected and how many potentially affected in a worst case scenario?	
5	What harm might be caused to individuals? The individuals do not necessarily need to be those whose personal data was involved in the breach. Harm shall be interpreted broadly, for example to include: distress; discrimination; loss of confidentiality; financial damage; identity theft; physical harm; and reputational damage.	

6	What harm might be caused to NST? For example, reputational damage and financial loss.	
7	What mitigating factors may have lessened the risks presented by the breach? The following questions may assist when considering this point. a. Were any physical protections in place to limit the impact of the breach e.g. was the data contained in a locked case when it was lost/stolen? b. Were any technical protections in place e.g. was the data protected by encryption? c. Have measures been taken to contain the breach e.g. have banks being notified where financial information has been compromised? d. Have measures been taken to recover the data e.g. has lost data been found before being seen by any unauthorised party or have back-ups been used where electronic information was lost or damaged?	

3. Notification to the Information Commissioner's Office

NST are required to report a data breach to the ICO unless the breach is unlikely to result in a risks to the rights and freedoms of individuals. The questions used to identify the risks will determine whether or not a breach needs to be reported to the ICO.

Any decision to not notify the ICO shall be documented. It is possible that if another data breach occurs in the future that the ICO will ask why any previous breaches were not reported and the ICO is likely to ask to see evidence of any decision to not notify. If a decision is made in conjunction with the CEO/COO to report a breach to the ICO this must be reported within 72 hours of the breach being recorded.

4. Content of the notification

The ICO has set out procedures for notifications on their website (ico.org.uk) which shall be followed. The notification must contain as a minimum:

- A description of the nature of the data breach including where possible:
- The categories and approximate number of data subjects concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer who can provide more information to the ICO if required;
- A description of the likely consequences of the data breach;
- A description of the measures taken or proposed to be taken by NST to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5. Contacting affected individuals

NST is required by the GDPR to report a data breach to the individuals whose data has been compromised (known as data subjects) where the breach is likely to result in a high risk to the rights and freedoms of individuals. It may not always be clear which individuals shall be notified, for example, parents may need to be notified rather than their children.

NST shall work with the ICO in determining when is the most appropriate time to notify the individuals. Other outside agencies, such as the police, may also have a view regarding the timing of this notification.

6. Content of the notification to individuals

- The notification to individuals must include the following as a minimum:
- The name and contact details of the Data Protection Officer who can provide more information;
- A description of the likely consequences of the data breach; and
- A description of the measures taken or proposed to be taken by NST to address the data breach, including,
- Where appropriate, measures to mitigate its possible adverse effects.
- The notification must be drafted in clear language. If directed at pupils/students the notification shall be age appropriate.

7. Serious Incident Report to the Education and Skills Funding Agency

An academy trust's funding agreement makes it clear that the Charity Commission's guidance on serious incident reporting must be followed by academies and, accordingly, that serious incidents shall be reported to the Education and Skills Funding Agency, as the principal regulator of academies, as soon as possible. Where there has been a data breach, NST will need to consider whether to make a serious incident report to the Education and Skills Funding Agency.

Trustees shall consider the Charity Commission's guidance on reporting serious incidents and in particular, the examples of what to report in the "Data breaches or loss" section of their table of examples.

The Education and Skills Funding Agency has extensive information sharing powers with other regulators, like the ICO, so the Education and Skills Funding Agency may be aware if a serious incident report is not made. This does not absolve NST of the obligation to make a serious incident report; rather it increases the likelihood of the Education and Skills Funding Agency detecting a failure to do so.

Because of the breadth of the Charity Commission's criteria for making serious incident reports, Trustees shall consider whether to make a report in light of the data breach and surrounding circumstances - even where it has not been necessary to notify the ICO.

8. Notification to the police

NST shall consider whether the police need to be notified about the data breach because it is possible that a criminal offence has been committed. However, there is no legal obligation to notify the police. The following are examples of breaches where a criminal offence may have been committed:

- theft e.g. if a laptop has been stolen;
- burglary;
- If a staff member has shared or accessed personal data where this was not required as part of their professional duties e.g. A staff member shares information about a pupil with famous parents with the local press;
- NST's computer network has been hacked (e.g. By a pupil/student or a third party).
- Action fraud is the national fraud and cybercrime reporting centre. It can be contacted on 0300 123 2040 or using www.actionfraud.police.uk

Appendix B: Examples of breaches

We will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach

Example	Remedial Action	Notification
A staff member leaves papers containing information about pupils' academic performance on a train. The papers were not in a locked case.	NST shall find out if it is possible to retrieve the papers. For example, by calling the train company's lost property department.	If the papers are not retrieved then this breach will need to be notified to the ICO. Whether a notification to the pupils/students and their parents/carers is required will depend upon the nature of the personal data. NSTT shall consult section 7 of this policy.
Ransomware locks electronic files containing personal data.	NST shall have a back-up of the data and shall also ensure that its systems are secured (e.g. that the ransomware has been removed).	Depends on factors such as whether NST was able to recover the data and whether there is any other risk to NST's systems.
Sending an email containing personal data to the incorrect recipient.	Use the recall email feature if available. Consider calling the unintended recipient and asking them to delete the email. Request that the recipient of the email confirm in writing that the information has been deleted.	Depends on the sensitivity of any personal data contained in the email, whether the unintended recipient has agreed to delete it etc.

Appendix C: Staff Guidance- Personal Data

Personal Data

The following are **examples** of the information that falls within the scope of this policy;

- Data protection concerns information about individuals;
- Personal Data is data which relates to a living person who can be identified either from that data, or from the data and other information that is available.
- Information as simple as someone's name and address is their Personal Data;
- In order for you to do your job, you will need to use and create Personal Data. Virtually anything might include Personal Data.

Examples of **places** where Personal Data might be found are:

- On a computer database;
- In a file, such as a pupil report;
- A register or contract of employment;
- Pupils' exercise books, coursework and mark books;
- Health records; and
- Email correspondence.

Examples of **documents** where Personal Data might be found are:

- A report about a child protection incident;
- A record about disciplinary action taken against a member of staff;
- Photographs/images of pupils/students;
- Tape recording of a job interview;
- Contact details and other personal information held about pupils, parents and staff and their families;
- Contact details of a member of the public who is enquiring about placing their child at the school;
- Financial records of a parent/carer;
- Information on a pupil's/student's performance; and
- An opinion about a parent/carer or colleague in an email.

Categories of Critical Personal Data

The following categories are referred to as Critical Personal Data in this policy and in the Telecommunications and Computer Use policy. You must be particularly careful when dealing with Critical Personal Data which falls into any of the categories below:

- Information concerning child protection matters;
- Information about serious or confidential medical conditions and information about special educational needs;
- Information concerning serious allegations made against an individual (whether or not the allegation amounts to a criminal offence and whether or not the allegation has been proved);
- Financial information (for example about parents and staff);
- Information about an individual's racial or ethnic origin;
- Political opinions;
- Religious beliefs or other beliefs of a similar nature;
- Trade union membership;
- Physical or mental health or condition; sex life or sexual orientation;
- Genetic information;
- Information relating to actual or alleged criminal activity;
- Biometric information (e.g. a pupil's fingerprints following a criminal investigation).

Appendix D: Staff Guidance- Sharing Personal Data

i. Personal Data must be processed fairly, lawfully and transparently

What does this mean in practice?

"Processing" covers virtually everything which is done in relation to Personal Data, including using, disclosing, copying and storing Personal Data;

Individuals must be told what data is collected about them, what it is used for, and who it might be shared with, unless it is obvious. They must also be given other information, such as, what rights they have in their information, how long we keep it for and about their right to complain to the Information Commissioner's Office (ICO, the data protection regulator). This information is often provided in a document known as a privacy notice or a transparency notice. Copies of the NST's privacy notices can be obtained from the NST websites. You must familiarise yourself with NST's pupil/student, parent/carer and staff privacy notices.

If you are using Personal Data in a way which you think an individual might think is unfair please speak to the DPL or DPO.

You must only process Personal Data for the following purposes:
a. Ensuring that NST provides a safe and secure environment;
b. Providing pastoral care;
c. Providing education and learning for our pupils/students;
d. Providing additional activities for pupils/students and parents/carers (for example activity clubs);
e. Protecting and promoting the NST's interests and objectives (for example fundraising);
f. Safeguarding and promoting the welfare of our pupils/students; and
g. To fulfil NST's contractual and other legal obligations.

If you want to do something with Personal Data that is not on the above list, or is not set out in the relevant privacy notice(s), you must contact the DPL/DPO. This is to make sure that NST has a lawful reason for using the Personal Data.

We may sometimes rely on the consent of the individual to use their Personal Data. This consent must meet certain requirements and therefore you should contact the DPL/DPO if you think that you may need to obtain consent.

ii. You must only process Personal Data for limited purposes and in an appropriate way.

What does this mean in practice?

For example, if pupils/students are told that they will be photographed to enable staff to recognise them when writing references, you should not use those photographs for another purpose (e.g. in NST's prospectus).

iii. Personal Data held must be adequate and relevant for the purpose

What does this mean in practice?

This means not making decisions based on incomplete data. For example, when writing reports you must make sure that you are using all of the relevant information about the pupil/student.

iv. You must not hold excessive or unnecessary Personal Data

What does this mean in practice?

Personal Data must not be processed in a way that is excessive or unnecessary. For example, you should only collect information about a pupil's/student's medical history if that Personal Data has some relevance, such as allowing NST to care for the pupil/student and meet their medical needs.

v. The Personal Data that you hold must be accurate

What does this mean in practice?

You must ensure that Personal Data is complete and kept up to date. For example, if a parent/carer notifies you that their contact details have changed, you should update NST's information management system.

vi. You must not keep Personal Data longer than necessary

What does this this mean in practice?

NST has a Retention Policy about how long different types of data should be kept for and when data should be destroyed. This applies to both paper and electronic documents. You must be particularly careful when you are deleting data. Please contact the DPL/DPO if you require further guidance on the retention periods and secure deletion.

vii. You must keep Personal Data secure

You must comply with the following policies and guidance relating to the handling of Personal Data:

i. ICT Acceptable Use policy;
ii. Staff Code of Conduct:
iii. Retention Policy; and
iv. Child Protection and Safeguarding Policy.

You must not transfer Personal Data outside the EEA without adequate protection

What does this mean in practice?

If you need to transfer personal data outside the EEA please contact the DPL/DPO. For example, if you are arranging a school trip to a country outside the EEA.

Sharing Personal Data outside of NST - dos and don'ts

Please review the following dos and don'ts:

i. **DO share Personal Data on a need to know basis** - think about why it is necessary to share data outside of the Trust - if in doubt - always ask the DPL/DPO.

ii. **DO encrypt emails which contain Critical Personal Data** described in section 3 above. For example, encryption should be used when sending details of a safeguarding incident to social services.

iii. **DO make sure that you have permission from the DPL/DPO to share Personal Data on the website**.

iv. **DO be aware of "blagging".** This is the use of deceit to obtain Personal Data from people or organisations. You should seek advice from the DPL/DPO where you are suspicious as to why the information is being requested or if you are unsure of the identity of the requester (e.g. if a request has come from a parent/carer but using a different email address).

v. **DO be aware of phishing**. Phishing is a way of making something (such as an email or a letter) appear as if it has come from a trusted source. This is a method used by fraudsters to access valuable personal details, such as usernames and passwords. Don't reply to email, text, or pop-up messages that ask for

personal or financial information or click on any links in an email from someone that you don't recognise. Report all concerns about phishing to the IT department.

vi. **DO NOT disclose Personal Data to the Police without permission from the DPL/DPO (unless it is an emergency).**

vii. **DO NOT disclose Personal Data to contractors without permission from the DPL/DPO.** This includes, for example, sharing Personal Data with an external marketing team to carry out a pupil/student recruitment event.

Sharing Personal Data within NST

This section applies when Personal Data is shared within NST. Personal Data must only be shared within NST on a "need to know" basis.

Examples of sharing which are likely to comply with the data protection legislation:

- A teacher discussing a pupil's/student's academic progress with other members of staff (for example, to ask for advice on how best to support the pupil/student);
- Informing an exam invigilator that a particular pupil/student suffers from panic attacks; and disclosing details of a teaching assistant's allergy to bee stings to colleagues so that you/they will know how to respond (but more private health matters must be kept confidential).

Examples of sharing which are unlikely to comply with the data protection legislation:

- Informing all staff that a pupil/student has been diagnosed with dyslexia (rather than just informing those staff who teach the pupil/student); and
- Disclosing personal contact details for a member of staff (e.g. Their home address and telephone number, birthday) to other members of staff (unless the member of staff has given permission or it is an emergency).

You may share Personal Data to avoid harm, for example in child protection and safeguarding matters. NST has a Child Protection and Safeguarding Policy which should be referred to. You should have received training on when to share information regarding welfare and safeguarding issues. If you have not received this training please let your line manager know as a matter of urgency.

Individuals' rights in their Personal Data

People have various rights in their information. You must be able to recognise when someone is exercising their rights so that you can refer the matter to the DPL/DPO. These rights can be exercised either in writing (e.g. in an email) or orally.

Please let the DPL/DPO know if anyone (either for themselves or on behalf of another person, such as their child):

i. Wants to know what information NST holds about them or their child;
ii. Asks to withdraw any consent that they have given to use their information or information about their child;
iii. Wants NST to delete any information;
iv. Asks NST to correct or change information (unless this is a routine updating of information such as contact details);
v. Asks for electronic information which they provided to NST to be transferred back to them or to another organisation;
vi. Wants NST to stop using their information for direct marketing purposes. Direct marketing has a broad meaning for data protection purposes and might include communications such as the Trust newsletter or alumni events information; or
vii. Objects to how NST is using their information or wants NST to stop using their information in a particular way, for example, if they are not happy that information has been shared with a third party

Appendix E: Staff Guidance- Subject Access Requests

One of the most commonly exercised rights is the right to make a subject access request. Under this right people are entitled to request a copy of the Personal Data which NST holds about them (or in some cases their child) and to certain supplemental information.

Subject access requests do not have to be labelled as such and do not even have to mention data protection.

For example, an email which simply states "Please send me copies of all emails you hold about me" is a valid subject access request. You must always immediately let the DPL/DPO know when you receive any such requests.

Receiving a Subject Access Request is a serious matter for NST and involves complex legal rights. Staff must never respond to a Subject Access Request themselves unless authorised to do so.

When a subject access request is made, NST must disclose all of that person's Personal Data to them which falls within the scope of his/her request - there are only very limited exceptions. There is no exemption for embarrassing information - so think carefully when writing letters and emails as they could be disclosed following a subject access request. However, this should not deter you from recording and passing on information where this is appropriate to fulfil your professional duties, particularly in relation to safeguarding matters.

You must act on the Subject Access Request without undue delay and at the latest within one calendar month of receipt. A calendar month starts on the day after the organisation receives the request, even if that day is a weekend or public holiday. You should calculate the time limit from the day after you receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.