General Data Protection Regulations (GDPR)

Nottingham Schools Trust Data Protection Policy

January 2021

Data Protection Policy

Contents

1. Introduction
2. Definitions
3. Policy aim
4. Policy objective
5. Processing of information
6. What counts as personal information
7. Processing of special categories of personal information
8. Access to information
9. Fair Obtaining/Processing
10. Data Uses and Purposes
11. Data Incident Reporting/ Data Breach
12. Data Quality and Retention
13. Records of processing activities
14. Data Security

This policy will be reviewed January 2022

Data Protection Policy

1. Introduction

Nottingham Schools Trust aims to ensure that personal information is treated in a lawful, fair and transparent manner. The lawful and correct treatment of personal information is extremely important in maintaining the confidence of those with whom the NST deals and in achieving its objectives. This policy sets out the basis on which we shall process any personal data from Member schools, SIAs, Trustees, staff, Nottingham City Council and other parties from whom data is collected.

We, and therefore any person who handles personal data on behalf of NST, fully endorses and adheres to the data protection principles set out in Article 5 of the GDPR and sections 83-89 DPA 2018 as below and shall be responsible for and be able to demonstrate compliance with the principles outlined below:-

THE SEVEN DATA PROTECTION PRINCIPLES

Personal Information shall be:

- processed lawfully, fairly and in a transparent manner **(lawfulness, fairness and transparency)**
- collected for specified explicit and legitimate purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;**(purpose limitation)**
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;**(data minimisation)**
- accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay **(accuracy)**
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required to safeguard the rights and freedoms of the data subject (**storage limitation**)
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (**integrity and confidentiality**)

- kept in a responsible manner and compliance is demonstrated by ensuring there are appropriate measures and records in place along with compliance of all data principles **(accountability)**

2. Definitions

Personal data

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

Personal data breach

Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, access to personal data transmitted, stored or otherwise processed.

Consent

Means any freely given, specific, informed and unambiguous indication of wishes, by a statement or clear affirmative action which signifies agreement to the processing of data.

Special categories of personal data

Is personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning a natural persons sex life or sexual orientation.

Processing

Includes any operation or set of operations, whether or not by automated means such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, use, disclosure, erasure or destruction.

Subject Access Request

Right to access personal data by any data subject for whom personal data is held by NST.

Data subject

This will be the person that we collect the data from and about. This will include member schools, SIAs, Trustees, NST staff and Nottingham City Council and any external providers and partners who do business with NST.

3. Policy Aim

To ensure NST complies with all relevant legislation and good practice to protect all of the personal information that it holds.

4. Policy Objectives

To achieve the overall aim NST will:

- Provide adequate resources to support an effective approach to data protection.
- Respect the confidentiality of all personal information irrespective of source.
- Publicise the Trust's commitment to Data Protection.
- Compile and maintain appropriate procedures and codes of practice.
- Promote general awareness and provide specific training, advice and guidance to its staff and associates at all levels to ensure standards are met.
- Monitor and review compliance with legislation and introduce changes to policies and procedures where necessary.

5. Processing of Information

By using appropriate management controls when processing personal information about any individual, we will:

- Observe fully the conditions regarding the collection and use of information and meet NSTs legal obligations under the GDPR and the Data Protection Act 2018.

- Collect and process appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

- Ensure that the individual about whom information is held can exercise their rights under the Act unless an exemption applies, for example in relation to education data, including the right:-

  - to be informed that processing is being undertaken
  - to prevent processing in certain circumstances
  - to correct, rectify, block or erase information, which is regarded as incorrect information
  - to access personal information
  - to erasure
  - to portability where applicable.

6. What counts as Personal Information?

This is any information held by NST about a living individual, from which that individual can be identified. For example, this includes:

- A name and address or contact details
- characteristics such as ethnicity, language, nationality, country of birth,
- information attached to a reference number that could be used to identify someone
- photographs
- financial records relating to an individual
- staff employment records

7. Processing of special categories of personal Information

We, through appropriate management controls will, when processing special categories of personal information about any individual:

- Observe fully the conditions regarding the processing of special categories of information as outlined in Article 9 and meet NST's legal obligations under the GDPR and the Data Protection Act 2018. In particular, Schedule 1 Part 4 of the DPA 2018 states that NST must have this policy document in place which explains as below, the procedures for securing compliance with the principles in Article 5 as outlined above.

- Collect and process special categories of data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirement.

- Process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs data, data concerning health or data concerning a natural person or trade union membership and the processing of genetic data and biometric data for the purpose of uniquely identifying a natural person.

8. Access to Personal Information

NST will process requests for access to personal information in line with the relevant sections of the GDPR and the Data Protection Act 2018.

Subject Access Requests

Individuals can request a copy of the personal data NST holds about them by contacting to the Data Protection Officer for the NST.

- if all information has been received, and the request is a valid subject access request, NST will acknowledge the request and process the request within 30 days from receipt, unless the request is particularly large and complex in which case the time can be extended for two months.

Requests from other agencies for personal information

- Requests from any external agency will be processed in accordance with the GDPR 2017 and Data Protection Act 2018.
- The DPO will ensure that any disclosure made without the consent of the data subject is done in accordance with the data protection and other relevant legislation, taking account of an individual's rights as enshrined in the Human Rights Act 1998. Relevant, confidential information should only be disclosed to:
  - other members of staff on a need to know basis
  - other authorities if it is necessary in the public interest, e.g. prevention of crime

9. Fair Obtaining/Processing

Individuals whose information is collected by NST must be made aware at the time of collection of all the processes that data may be subject to. No manual or automatic processing of personal information will take place unless reasonable steps have been taken to make that individual aware of that processing. Data subjects will also be informed of likely recipients of their information, both internal and external, and also be given details of who to contact in order to query the use or content of their information. Data subjects will also be informed of the purposes of the processing as well as the legal basis for processing where appropriate.

Information as to how long the information will be kept for, the rights that the data subject can exercise with regards to their data and information to enable them lodge a complaint with the Information Commissioners Office if their rights are not met under the GDPR and DPA 2018 can be provided on request.

10. Data Uses and Purposes

All processing of personal data must be for a purpose that is necessary to enable NST to perform its duties and services. Personal information should only be processed in line with those notified purposes.

All personal data will be regarded as confidential and its security protected accordingly. This also applies when NST information is being processed off site, including on mobile devices. Information held by NST must not be used for unauthorised non-NST purposes. If you become aware of any potential data breach, please refer to section 11 below, and follow the designated procedures accordingly.

Personal Information should only be disclosed to persons (internal and external) where their authority to receive it has been explicitly established, e.g. a relevant Information Sharing Agreement or Consent Form is in place, or where the information is required by the police for the prevention and detection of crime.

11. Data Incident Reporting / Data Breach

The Data Protection Officer must be informed of any potential data incidents as soon as the incident occurs and in any event within 24 consecutive hours after occurrence. Any reported data incident will be investigated appropriately and actions taken as necessary.

If a member of the public reports a potential incident, they can do this by contacting the Data Protection Officer directly by phone on 0115 915 3701 or by e-mail on dpo@nottinghamschoolstrust.org.uk

Personal data breaches will be notified to the Information Commissioner's Office within 72 hours of the incident. All staff, Associates and any other person working on behalf NST will follow the NST's Data Incidents and Breaches policy. Further information can be found on the ICO Website.

12. Data Quality and Retention

Whenever information is processed, reasonable steps should be taken to ensure that it is up to date and accurate.

Information processed should not be excessive or irrelevant to the notified purposes.

Information must be held only for so long as is necessary for the notified purposes, after which it should be deleted or destroyed in accordance with the NST Retention Policy.

13. Records of processing activities

In order to be able to properly and effectively comply with our obligations under the GDPR and the DPA2018, NST needs to fully understand what information it holds and where this information is kept. We also need to consider how we keep this information up-to-date and how we know when to dispose of it. NST shall maintain a record of processing which include the following information:

- The name of the Trust and the details of the Data Protection Officer
- The purposes of processing as outlined above in this policy document
- Which condition is relied on and in particular, how the processing satisfies Article 5 and 6
- Set out the ownership, governance and maintenance of Information Assets
- The Retention Policy
- Sets out whether the personal data is retained and erased in accordance with the policy and if it is not the reason for not following the policy
- Map the flow of data in and out of NST.

14. Data Security

NST must take all appropriate technical and organisational measures to safeguard against unauthorised or unlawful processing of personal information and against accidental loss, damage or destruction of personal information.

All personal information must be kept secure, in a manner appropriate to its sensitivity and the likely harm or distress that would be caused if it was disclosed unlawfully.

Everyone managing and handling personal information will be appropriately trained to do so and this will include appropriate refresher training every year.

All members of staff, Associates and any other person working on behalf of NST have a duty to follow this Policy and associated procedures and to co-operate with NST to ensure that the aim of this Policy is achieved.

All members of staff, Associates and any other person working on behalf of NST must be wary of possible threats the security of personal data, (e.g. computer screens being visible to members of the public who visit the site, etc.) and proactively take steps to mitigate the threats.

Disciplinary action may be taken against any member of staff who fails to comply with or commits a breach of this Policy.

It is the duty of individual members of staff to ensure that personal information held by them is dealt with in accordance with the Act.

Suitable measures should be taken to ensure that any processing of personal data carried out by a third party on behalf of NST complies with the Principles of the Act and this Policy. Similarly, when NST is processing personal information on behalf of a third party it will need to demonstrate that the information is subject to the same standard of care.

The Data Protection Policy should be read in conjunction with the following:

- Data Incidents and Breaches Policy
- Freedom of Information Policy
- Acceptable Use policy
- Email Policy
- Mobile Computing Policy
- Safeguarding Policy and Guidance

Copies of the above documents can be obtained by contacting the Data Protection Officer on

dpo@nottinghamschoolstrust.org.uk

Addendum

Statement on data protection and Brexit implementation – what you need to do (29th January 2020)

Update (13 July 2020): The UK left the EU on 31 January 2020 and is now in a transition period until 31 December 2020. Our end of transition guidance will help you to prepare for potential changes. We will keep our guidance under review, and update it as the situation evolves. There may be changes to how to receive personal data from the EU and action you may need to take on data protection. Please continue to monitor the ICO website over the transition period for these updates.

The UK will leave the European Union on 31 January and enter a Brexit transition period.

During this period, which runs until the end of December 2020, it will be **business as usual** for data protection.

The GDPR will continue to apply. Businesses and organisations that process personal data should continue to follow our existing guidance for advice on their data protection obligations.

During the transition period, companies and organisations that offer goods or services to people in the EU do not need to appoint a European representative. We have updated our Brexit FAQs to reflect this advice. The ICO will continue to act as the lead supervisory authority for businesses and organisations operating in the UK.

It is not yet known what the data protection landscape will look like at the end of the transition period and we recognise that businesses and organisations will have concerns about the flow of personal data in future.