Greater Nottingham Education Trust

Data Protection Policy

This policy will be reviewed by the Trust Board three yearly or amended if there are any changes in legislation before that time.

Date of last review: Autumn 2018
Date of next review: Autumn 2021

Contents

1. Aims 2
2. Definitions 2
3. The data controller 3
4. Processing personal data 3
5. Roles and responsibilities 3
6. Sharing personal data 4
7. Subject access requests and other rights of individuals 5
8. Parental requests to see the educational record 6
9. Biometric recognition systems 6
10. CCTV 6
11. Images 6
12. Data protection by design and default 7
13. Data security and storage of records 7
14. Disposal of records 7
15. Personal data breaches 7
16. Training 8

1. Aims

We aim to ensure that all personal data collected about employees, parents, governors, trustees, visitors, contractors and other adult individuals involved with our organisation (herein after known as staff) and pupils is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) . This policy applies to all personal data in all formats.

2. Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, 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/data which is regarded as sensitive information	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), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation It also means whether a child is looked-after, has SEND, or is eligible for free school meals.
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.
Subject Access Request (SAR)	An individual's request for information about the personal data held about them or for the data itself
Staff	All employees, governors, trainees, volunteers, trustees and any other adults working in or visiting the organization

3. The data controller

We process personal data relating to staff and pupils as defined above. In relation to some information the Greater Nottingham Education Trust (GNET) is a joint data controller with schools within the trust. GNET is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

4. Processing personal data

We respect every individual's privacy and personal information by:

- Processing personal data lawfully, fairly and transparently
- Collecting personal data for specified, explicit and legitimate reasons
- Holding and using no more personal data than we need
- Ensuring that the personal data we hold is accurate and kept up to date as necessary
- Anonymising personal data when we no longer need it to identify the individual
- Keeping all personal data safe and secure

We will only process personal data where we have 'lawful bases' (legal reasons) to do so under data protection law, including:

- The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent for the particular use or purpose

- The data needs to be processed to enable us to:
    - fulfil a contract with the individual, or the individual has asked us to take specific steps before entering into a contract
    - comply with a legal obligation
    - ensure the vital interests of the individual e.g. to protect someone's safety or life
    - perform a task in the public interest, and carry out its official functions
    - the data needs to be processed for the legitimate interests of the school or a third party (provided the individual's rights and freedoms are not overridden)

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

If we offer online services to pupils and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 or is not capable of understanding the consent process (except for online counselling and preventive services). Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law outlined in our privacy notice.

5. 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.

Trust Board

Trustees have overall responsibility for ensuring that the organisation complies with all relevant data protection obligations.

Data protection officer

The data protection officer (DPO) is responsible for monitoring our compliance with data protection law and is the point of contact for individuals whose data we process and for the ICO.

Our DPO is named on our website and can be contacted via dpo@gnetacademies.co.uk

Headteacher

The headteacher acts as the representative of the data controller on a day-to-day basis.

Staff

Staff must:

- Respect the privacy of all individuals and their personal information
- Collect, store, share and use all personal data only in accordance with this policy and the linked documents
- Only collect, store, share and use personal data where it is necessary in order to do their jobs or discharge their responsibilities.
- Not share personal data any more widely than necessary
- Ensure that personal data is anonymised or deleted once it is no longer needed, unless otherwise specified in the retention schedule
- Inform their school of any changes to their personal data, such as a change of address
- Contact the DPO :
    - If they have any questions about collecting, using, storing, sharing or securing personal data, their or the school's data protection obligations, the operation of this policy, data protection law or any other matter relating to data protection
    - Immediately they have any concerns that this policy or the linked policies are not being followed
    - Immediately they become aware of a data breach or a possible data breach
    - Immediately they receive any SAR as defined above or any other request relating to personal data.
    - If they are considering engaging in any new form of data processing
- Immediately contact the Designated Safeguarding Lead if a personal data breach or possible breach raises any safeguarding concerns

6. Sharing personal data

We will only share personal data where we need to do so, we are legally required to do so or we have consent. Circumstances in which we share personal data include where:

- There is a risk to which the safety of an individual
- We need to liaise with other agencies
- 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 data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share
    - Only share data that the supplier or contractor needs to carry out their service or which is necessary to keep them safe while working with us

and:

- For the prevention or detection of crime and/or fraud
- For the apprehension or prosecution of offenders
- For the assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Where there is an emergency

Where we 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. If we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law.

7. Subject access requests and other rights of individuals

Subject access requests

Individuals have a right to make a subject access request for information about the personal data which the school holds about them and for the data itself. All requests for information about or relating to an individual's personal data should be sent to our DPO at dpo@gnetacademies.co.uk. If staff receive a request for information about or relating to an individual's personal data they must immediately forward it to the DPO.

Children and subject access requests

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

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

Responding to subject access requests

When responding to requests, we:

- May ask the individual to provide two forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within one month of receipt of the request
- Will provide the information free of charge unless we deem the request to be manifestly unfounded or excessive
- May tell the individual we will comply within three months of receipt of the request, where a request is complex or numerous. We will inform the individual of this within one month, and explain why the extension is necessary

We will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Is given to a court in proceedings concerning the child
- Identifies a third party unless the third party has consented to the disclosure or it is reasonable to comply with the request without that person's consent.

If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee, which takes into account administrative costs. A request will be deemed unfounded or excessive if it is repetitive, or asks for further copies of the same information. When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

Other data protection rights of the individual

Individuals also have the right to:

- Be told of data processing (which is covered by our Privacy Notices)
- Object to or restrict the processing of personal information in certain circumstances
- Have inaccurate personal information rectified and, in certain circumstances, restricted, erased or destroyed
- Claim compensation for damages caused by a breach of the data protection regulations
- Withdraw consent
- Obtain and reuse their personal information for their own purposes across different services (data portability)
- Complain to the Information Commissioner's Office
- Prevent use of their personal data for direct marketing
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Be notified of a data breach in certain circumstances

Individuals should submit any request to exercise these rights to the DPO, except in the case of a complaint to Information Commissioner's Office. If staff receive such a request, they must immediately forward it to the DPO.

8. Parental requests to see the educational record

Parents, or those with parental responsibility, have a legal right to free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.

9. Biometric recognition systems

Where biometric recognition systems are in operation they use partial fingerprint to allow staff and pupils to purchase food and to check and top-up account balances within the cashless system. This is known as 'biometric data'. We will not use fingerprints in any other way or for any other purpose. We will only use biometric data if we have written consent. We will only use pupils' fingerprints if we have parental consent. If consent is not given for biometric access, we will provide suitable alternative access to these services. Biometric data is held securely within the organisation that it is used and will only be shared with the suppliers of our biometric identification systems. We will not unlawfully disclose it to any other person. When a pupil or member of staff leaves the organisation, or if consent for the use of the biometric system is withdrawn, the biometric data will be 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.

10. CCTV

Organisational specific CCTV policies set out how CCTV footage is used within that organisation.

11. Images

Organisational specific image policies set out how images are to be taken, stored and used within that organisation. Other linked policies and procedures which also refer to the taking, storing and use of images include:

- Acceptable use
- Child protection
- School and trip consent forms
- Staff code of conduct

12. Data protection by design and default

We will put measures in place to integrate 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 4)
- Completing privacy impact assessments where the 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
- Maintaining records of our processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our schools 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, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure

13. Data security and storage of records

Our separate staff acceptable use policy sets out how we 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.

14. Disposal of records

Personal data that is no longer needed will be disposed of securely or anonymised to preserve privacy. Personal data that has become inaccurate or out of date will also be disposed of securely or anonymised, 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.

15. Personal data breaches

Our data breach procedure sets out the action we will take in the event of a personal data breach or possible personal data breach. Where staff become aware of a personal data breach or possible breach, they must contact the DPO immediately. If the breach or possible breach raises any safeguarding concerns, staff must also immediately contact the Designated Safeguarding Lead (DSL).

16. Training

All staff 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.