Statutory
~~Non-Statutory~~

Data Protection Policy

Date January 2013
Reviewed September 2015
Reviewed May 2018

Northgate School Arts College Academy Trust

Data Protection Policy

Introduction

This policy applies to all employees, workers and contractors.

1. The Governing Body of Northgate School Arts College are committed to processing personal data (which may be held on paper, electronically, or otherwise) about our employees and we recognise the need to treat it in an appropriate and lawful manner, in accordance with the General Data Protection Regulation (GDPR). The purpose of this policy is to set out the principles by which we will handle your personal data.

2. Data users are obliged to comply with this policy when processing personal data on our behalf. Any breach of this policy may result in disciplinary action, including dismissal.

3. The Data Protection Officer (see point 17 for contact details) is responsible for ensuring compliance with the GDPR and this policy. Any questions about the operation of this policy or concerns that there has been a breach of this policy should be referred in the first instance to a member of the Senior Leadership Team.

1. Aims

Our school aims to ensure that all personal data collected about staff, pupils, parents, govenors, visitors and other individuals is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR) and the expected provisions of the Data Protection Act 2018 (DPA 2018) as set out in the Data Protection Bill.

This policy applies to all data, regardless of whether it is in paper or electronic format.

2. Legislation and guidance

This policy meets the requirements of the Data Protection Acct 1998, and is based on guidance published by the Information Commissioner's Office (ICO) and model privacy notices published by the Department for Education.

It also takes into account the provisions of the General Data Protection Regulation, which came into force in May 2018 and the ICO's code of practice for subject access requests. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

This policy complies with our funding agreement and articles of association.

3. Responsibilities

The Governing Body must:

- Manage and process personal data properly
- Protect the individual's rights to privacy
- Provide an individual with access to all personal information held on them.

The Governing Body have a legal responsibility to comply with the law, including the General Data Protection Regulation. The individual with overall responsibility for this policy is the Data Protection Officer.

The Governing Body are required to notify the Information Commissioner of the process of personal data; this is included in a public register. The public register of data controllers is available on the Information Commissioner's website.

The Governing Body's Data Protection Officer is responsible for drawing up guidance on good data protection practice and promoting compliance with the guidance through advising employees on the creation, maintenance, storage and retention of their records which contain personal information.

Every employee that holds, or has access to, information about identifiable living individuals must comply with data protection legislation in managing that information. All employees are responsible for acting in accordance with the policies, procedures and guidelines and within the provisions of the General Data Protection Regulation. **Individuals may be liable for breaches of the Regulation (See Appendix 1).**

4. Definitions

In this policy, unless otherwise stated or unless the context otherwise requires, each term will have the meaning set out below:

Data protection means practices and operations relating to the fair and lawful treatment of Personal Data and an understanding of the regulatory requirements relating to data privacy

Personal data is data which relates to a living individual who can be identified:
- From this data; or
- From this data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Examples of personal data can include, but are not limited to:
- Names
- Addresses
- Telephone numbers
- Dates of birth
- National Insurance numbers
- Employee numbers
- Named email addresses
- Account details
- CCTV images
- Photographs
- Personal opinions
- Internet browsing history
- Static/dynamic IP addresses

Examples of sensitive personal data can include, but are not limited to:
- Contact details
- Racial or Ethnic origin
- Political opinions
- Religious beliefs, or beliefs of a similar nature
- Where a person is a member of a trade union
- Physical and mental health
- Sexual orientation
- Whether a person has committed, or is alleged to have committed, an offence
- Criminal convictions

Data processing in relation to information of data, means obtaining, recording or holding the information/data or carrying out any operation or set of operations on the information/data, including:

- Organization, adaptation or alteration of the information/data
- Retrieval, consultation or use of the information/data
- Disclosure of the information or data by transmission, dissemination or otherwise making available
- Alignment, combination, blocking, erasure or destruction of the information or data; or
- Storage of information or data, whether electronically or manually (paper based).

Data subject is the person whose personal data is held or processed.

Data controller is a person or organization that determines the purposes for which, and the manner in which personal data is processed.

Data processor is a person, other than an employee of the data controller, who processes the data on behalf of the data controller.

5. The Data Controller

Our school processes personal information relating to pupils, staff and visitors, and therefore is a data controller. Our school delegates the responsibility of data controller to the School Business Manager.

The school is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

6. Data Protection Principles

The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling. In line with GDPR, anyone processing personal data must comply with the following principles. It is our policy that personal data must be:

- Processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed
- Personal data shall be accurate and, where necessary, kept up to date
- Personal data shall not be kept for longer than is necessary for the purpose(s) for which it is processed
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Acct 1998
- Appropriate technical and organizational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data.

7. Roles and Responsibilities

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

Governing Board

The governing board has overall responsibility for ensuring that our school complies with all relevant data protection obligations under the Data Protection Act 1998.

Day-to-Day responsibilities rest with the Executive Head Teacher, or Head of school in the Executive Head Teacher's absence. The Executive Head Teacher, will ensure that all staff are aware of their Data protection obligations, and oversee any queries relating to the storing or processing of personal data.

Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

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.

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.

Our DPO is Ruth and is contactable via Plumsun 0845 8622684.

The Executive Head Teacher acts as the representative of the data controller on a day-to-day basis.

Collecting Personal Data

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 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 e.g. 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**, 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)

- 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 which are set out in the GDPR and Data Protection Act 2018.

IF we offer online services to pupils, such as classroom apps, as we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13 (except for online counselling and preventative services).

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

Limitation, minimization 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 their jobs.

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 records management policy.

8. Privacy/Fair Processing Notice

8.1 Pupils and Parents

We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

This data includes, but is not restricted to:

- Contact details
- Results of internal assessment and externally set tests
- Data on pupil characteristics, such as ethnic group or special educational needs
- Exclusion information
- Details of any medical conditions

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

Personal data will be held in accordance with the Governing Body's p9olicy on Retention of personal Information. We will not keep personal data longer than necessary for the purpose or purposes for which they were collected. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required.

The Governing Body will state the purposes for which it holds personal information, and will register with the Data Protection Commissioner all the purposes for which it processes personal data.

We will not share information about pupils with anyone without consent unless the law or our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 9 and 10 of this policy.

Once our pupils reach the age of 13, we are legally required to pass on certain information to Northamptonshire Local Authority and Prospects who are the local careers service providers, who have responsibilities in relation to the education or training of 13-19 year olds. Parents, or pupils if aged 16 or over, can request that only their name, address and date of birth be passed on by informing the School Business Manager.

8.2 Staff

We process data relating to those we employ to work at, or otherwise engage to work at, our school. The purpose of processing this data is to assist in the running of the school, including to:

- Enable individuals to be paid
- Facilitate safe recruitment
- Support the effective performance management of staff
- Improve the management of workforce data across the sector
- Inform our recruitment and retention policies
- Allow better financial modelling and planning
- Enable ethnicity and disability monitoring
- Support the work of the School Teachers' Review Body

Staff personal data includes, but is not limited tom, information such as:

- Contact details
- National Insurance Numbers
- Salary information
- Qualifications
- Absence data
- Personal characteristics, including ethnic groups
- Medical information
- Outcomes of any disciplinary procedures

We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

We will not share information about staff with third parties without consent unless the law allows us to.

We are required, by law, to pass certain information about staff to specified external bodies, such as our local authority and the Department for Education, so that they are abl3e to meet their statutory obligations.

Any staff member wishing to see a copy of information about them that the school holds should contact the School Business Manager.

Sharing Personal Data

We will not normally share personal data with anyone else, but may do so 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 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, and information necessary to keep them safe while working with us

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

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy our safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

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

9. Subject Access Requests

Under the Data Protection Act 1998, pupils have a right to request access to information the school holds about them. This is known as a subject access request.

Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The pupil's name
- A correspondence address
- A contact number and email address
- Details about the information requested

The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interests
- Information contained in adoption and parental order records
- Certain information given to a court in proceedings concerning the child

Subject access requests for all or part of the pupil's educational record will be provided within 15 school days. The table below summarises the charges that apply:

Number of pages of information to be supplied	Maximum fee (£)
1-19	1.00
20-29	2.00
30-39	3.00
40-49	4.00
50-59	5.00

60-69	6.00
70-79	7.00
80-89	8.00
90-99	9.00
100-149	10.00
150-199	15.00
200-249	20.00
250-299	25.00
300-349	30.00
350-399	35.00
400-449	40.00
450-499	45.00
500+	50.00

If the subject access request does not relate to the educational record, we will respond within 40 calendar days. The maximum charge that will apply in this instance will be £10.00

10. Parental requests to see the educational record

Parents of pupils at this school do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such requests, and we will bear in mind guidance issued from time to time from the Information Commissioner's Office (the organisation that upholds information rights).

11. Storage of Records

- Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use
- Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access
- Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office
- Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals
- 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 for school-owned equipment.

12. Disposal of Records

Personal information that is no longer needed, or has become inaccurate or out of date, is disposed of securely.

For example, we will shred or incinerate paper-based records, and override electronic files. We may also use an outside company to safely dispose of electronic records.

13. Training

Our 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 or the school's processes make it necessary.

14. References

The Governing Body will comply with the DfE guidance on references as amended from time to time, in particular in relation to safeguarding children and safer recruitment in education.

15. Review of the Policy

This policy shall be reviewed as necessary. We reserve the right to change this policy at any time. Where appropriate, we will notify data subjects of those changes by mail, email and/or staff notice board.

16. Related Documents

This policy is supported by the following documents:

- Subject Access Request Policy
- IT Acceptable Use Policy
- Privacy Notices
- Data Retention Policy
- Code of Conduct/Disciplinary Policy

17. Relevant Contacts

Data Protection Officer
Please refer any queries, issues or requests received to the Data Protection Officer

Ruth Hawker
Company Director
Plumsun Ltd
4 Pavilion Court
600 Pavilion Drive
Northampton Business Park
Northampton
NN4 7SL

ICO contact details
If you require more information about the General Data Protection Regulations, the Data Protection Bill, or are unhappy with the way we have dealt with your data, please contact:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

www.ico.org.uk

Appendix 1: Personal Data Breach Procedure

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

- On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO.
- 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
- The DPO will alert the Head Teacher and the Chair of Governors.
- The DPO will make all reasonable efforts to contain and minimize the impact of the breach, assisted by relevant staff members or data processors where necessary. (Actions relevant to specific data types are set out 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.
- The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned

  If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.

- The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the school's computer system.

- Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website within 27 hours. 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. 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.

- The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If this risk is high, the DPO will promptly inform, in writing, all individuals whose personal data has been breached. This notification will set out:

    - 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 notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, bank 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 on the school's computer system.

- The DPO and Head Teacher 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 will take the actions set out below to mitigate the impact of different types of data breach, focusing especially on breaches involving particularly risk 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 to recall it*
- *If any cases where the recall is unsuccessful, the DPO will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and the request that those individuals delete the information and do not share, publish, save or replicate it in any way*
- *The DPO will ensure we receive 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 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*

Other types of data breaches:

- *Details of pupil premium interventions for named children being published on the school website*
- *Non-annoymised pupil exam results of 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*