Northern Arch
LEARNING PARTNERSHIP

Trust GDPR Data Protection Policy

Approved by: Board of Directors

Review frequency: 1 year

Date of last review: Spring 2026

Date of next review: Spring 2027

1. Statement of Intent

1.1. Northern Arch Learning Partnership is required to keep and process certain information about its staff members and pupils in accordance with its legal obligations under the UK GDPR.

1.2. The Academy/Trust may, from time to time, be required to share personal information about its staff or pupils with other organisations, mainly the LA, other schools and educational bodies, and potentially children's services.

1.3. This This policy is in place to ensure all staff and governors are aware of their responsibilities and outlines how the Academy/Trust complies with the following core principles of the UK GDPR.

1.4. Organisational methods for keeping data secure are imperative, and Northern Arch Learning Partnership believes that it is good practice to keep clear practical policies, backed up by written procedures.

1.5. This policy complies with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, together forming the primary data protection legislation in the UK.

2. Legal framework

2.1. This policy has due regard to legislation, including, but not limited to the following:

- The General Data Protection Regulation
- The Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998 This policy also has regard to the following guidance:
    - ICO (2018) 'Guide to the General Data Protection Regulation (GDPR)

2.2. This policy will be implemented in conjunction with the following other Academy/Trust policies:

- Freedom of Information Policy
- IT Acceptable User Policy
- Safeguarding Policy
- Code of Conduct for employees Policy
- Capability Policy
- Whistleblowing Policy
- Grievance Policy
- Data Retention & Destruction Policy
- CCTV Policy (where applicable)
- Employees working remotely and Bring your own Devices to Work Policy

3. Applicable Data

3.1. For the purpose of this policy, **personal data** refers to information that relates to an identifiable, living individual, including information such as an online identifier, e.g. an IP address. The UK GDPR applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well

3.2. **Sensitive personal data** is referred to in the UK GDPR as 'special categories of personal data', which are broadly the same as those in the Data Protection Act (DPA) 1998. These specifically include the processing of genetic data, biometric data and data concerning health matters.

4. Principles

4.1. In accordance with the requirements outlined in the UK GDPR, personal data will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- 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.
- 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, insofar 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 by the UK GDPR in order to safeguard the rights and freedoms of individuals.
- 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.
- Personal data will not be transferred internationally unless appropriate safeguards are in place in accordance with the UK's international data transfer regime (UK GDPR Chapter V).
- The UK GDPR also requires that "the controller shall be responsible for, and able to demonstrate, compliance with the principles".

5. Accountability

5.1. Northern Arch Learning Partnership will implement appropriate technical and organisational measures to demonstrate that data is processed in line with the principles set out in the UK GDPR.

5.2. The Academy/Trust will provide comprehensive, clear and transparent privacy policies to all stakeholders.

5.3. Records of activities relating to higher risk processing will be maintained, such as the processing of activities that:

- Are not occasional.
- Could result in a risk to the rights and freedoms of individuals.
- Involve the processing of special categories of data or criminal conviction and offence data.
- Internal records of processing activities will include the following:
- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place
- The Academy/Trust will implement measures that meet the principles of data protection by design and data protection by default, such as:
- Data minimisation.
- Pseudonymisation.
- Transparency.
- Allowing individuals to monitor processing.
- Continuously creating and improving security features.
- Data protection impact assessments will be used, where appropriate.

6. Roles and Responsibilities

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

6.2. Governing Board

The Northern Arch Learning Partnership Board of Directors and the academy's Local Governing Bodies have overall responsibility for ensuring that all academies comply with all relevant data protection obligations.

6.3. Data Protection Officer (DPO)

Northern Arch Learning Partnership's Data Protection Officer is S Jones, who is contactable through SJones@nalp.org.uk

6.4. The DPO will Inform and advise the school and its employees about their obligations to comply with the GDPR and other data protection laws.

6.5. Monitor the school's compliance with the UK GDPR and other laws, including managing internal data protection activities, advising on data protection impact assessments, conducting internal audits, and providing the required training to staff members.

6.6. An existing employee will be appointed to the role of DPO provided that their duties are compatible with the duties of the DPO and do not lead to a conflict of interests.

6.7. The DPO will report to the highest level of management at the Trust

6.8. The DPO will operate independently and will not be dismissed or penalised for performing their task.

6.9. Sufficient resources will be provided to the DPO to enable them to meet their UK GDPR obligations

6.10. Data Controller

6.11. Northern Arch Learning Partnership processes personal data relating to parents, pupils, staff, governors, visitors and others, and therefore is a data controller.

6.12. The Academy/Trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

6.13. The Principal/Head Teacher/Head of School acts as the representative of the data controller on a day to-day basis.

6.14. All Staff

Staff are responsible for:

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

6.15. 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 or suspect a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals

7. Lawful Processing

7.1. The legal basis for processing data will be identified and documented prior to data being processed.

7.2. Under the UK GDPR, data will be lawfully processed under the following conditions:

- The consent of the data subject has been obtained.
- Processing is necessary for:
  - Compliance with a legal obligation.
  - The performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
  - For the performance of a contract with the data subject or to take steps to enter into a contract.
  - Protecting the vital interests of a data subject or another person.
  - For the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject. (This condition is not available to processing undertaken by the Academy/Trust in the performance of its tasks.) Sensitive data will only be processed under the following conditions:
  - Explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law.
  - Processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent.
  - Processing relates to personal data manifestly made public by the data subject.
- Processing is necessary for:
  - Carrying out obligations under employment, social security or social protection law, or a collective agreement.
  - Protecting the vital interests of a data subject or another individual where the data subject is physically or legally incapable of giving consent.
  - The establishment, exercise or defence of legal claims or where courts are acting in their judicial capacity.
  - Reasons of substantial public interest on the basis of Union or Member State law which is proportionate to the aim pursued and which contains appropriate safeguards.
  - The purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of

health or social care systems and services on the basis of Union or Member State law or a contract with a health professional.

- Reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices.
- Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with article 89(1).

8. Consent

8.1. Consent must be a positive indication. It cannot be inferred from silence, inactivity or pre-ticked boxes.

8.2. Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes.

8.3. Where consent is given, a record will be kept documenting how and when consent was given.

8.4. The school ensures that consent mechanisms meet the standards of the UK GDPR. Where the standard of consent cannot be met, an alternative legal basis for processing the data must be found, or the processing must cease.

8.5. Consent accepted under the DPA will be reviewed to ensure it meets the standards of the UK GDPR; however, acceptable consent obtained under the DPA will not be reobtained

8.6. Consent can be withdrawn by the individual at any time.

8.7. Where a child is under the age of 13, parental consent will be sought prior to the processing of their data, except where the processing is related to preventative or counselling services offered directly to a child.

9. The right to be informed

9.1. The privacy notice supplied to individuals in regards to the processing of their personal data will be written in clear, plain language which is concise, transparent, easily accessible and free of charge.

9.2. If services are offered directly to a child, the school will ensure that the privacy notice is written in a clear, plain manner that the child will understand.

9.3. In relation to data obtained both directly from the data subject and not obtained directly from the data subject, the following information will be supplied within the privacy notice:

- The identity and contact details of the controller (and where applicable, the controller's representative) and the DPO.
- The purpose of, and the legal basis for, processing the data.
- The legitimate interests of the controller or third party.
- Any recipient or categories of recipients of the personal data.

- Details of transfers to third countries and the safeguards in place.
- The retention period of criteria used to determine the retention period.
- The existence of the data subject's rights, including the right to:
  - Withdraw consent at any time
  - Lodge a complaint with a supervisory authority.

9.4. Where data is obtained directly from the data subject, information regarding whether the provision of personal data is part of a statutory or contractual requirement, as well as any possible consequences of failing to provide the personal data, will be provided.

9.5. Where data is not obtained directly from the data subject, information regarding the categories of personal data that the Academy/Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.

9.6. For data obtained directly from the data subject, this information will be supplied at the time the data is obtained

9.7. In relation to data that is not obtained directly from the data subject, this information will be supplied:

- Within one month of having obtained the data.
- If disclosure to another recipient is envisaged, at the latest, before the data are disclosed.
- If the data are used to communicate with the individual, at the latest, when the first communication takes place.

10. The right of access

10.1. The have the right to obtain confirmation that their data is being processed.

10.2. Individuals have the right to submit a subject access request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing.

10.3. The Academy/Trust will verify the identity of the person making the request before any information is supplied.

10.4. A copy of the information will be supplied to the individual free of charge; however, the Academy/Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information.

10.5. Where a SAR has been made electronically, the information will be provided in a commonly used electronic format.

10.6. Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged.

10.7. All fees will be based on the administrative cost of providing the information.

10.8. All requests will be responded to without delay and at the latest, within one month of receipt.

10.9. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this

extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

10.10. Where a request is manifestly unfounded or excessive, the Academy/Trust holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the supervisory authority and to a judicial remedy, within one month of the refusal.

10.11. In the event that a large quantity of information is being processed about an individual, the Academy/Trust will ask the individual to specify the information the request is in relation to.

11. The right to rectification

11.1. Individuals are entitled to have any inaccurate or incomplete personal data rectified.

11.2. Where the personal data in question has been disclosed to third parties, the Academy/Trust will inform them of the rectification where possible.

11.3. Where appropriate, the Academy/Trust will inform the individual about the third parties that the data has been disclosed to.

11.4. Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.

11.5. Where no action is being taken in response to a request for rectification, the Academy/Trust will explain the reason for this to the individual and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

12. The right to erasure

12.1. Individuals hold the right to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

12.2. Individuals have the right to erasure in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- When the individual withdraws their consent
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed
- The personal data is required to be erased in order to comply with a legal obligation
- The personal data is processed in relation to the offer of information society services to a child

12.3. The Academy/Trust has the right to refuse a request for erasure where the personal data is being processed for the following reasons:

- To exercise the right of freedom of expression and information

- To comply with a legal obligation for the performance of a public interest task or exercise of official authority
- For public health purposes in the public interest
- For archiving purposes in the public interest, scientific research, historical research or statistical purposes
- The exercise or defence of legal claims

12.4. As a child may not fully understand the risks involved in the processing of data when consent is obtained, special attention will be given to existing situations where a child has given consent to processing and they later request erasure of the data, regardless of age at the time of the request.

12.5. Where personal data has been disclosed to third parties, they will be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

12.6. Where personal data has been made public within an online environment, the Academy/Trust will inform other organisations who process the personal data to erase links to and copies of the personal data in question.

13. The right to restrict processing

13.1. Individuals have the right to block or suppress the Academy/Trust's processing of personal data.

13.2. In the event that processing is restricted, the Academy/Trust will store the personal data, but not further process it, guaranteeing that just enough information about the individual has been retained to ensure that the restriction is respected in future.

13.3. The Academy/Trust will restrict the processing of personal data in the following circumstances:

- Where an individual contests the accuracy of the personal data, processing will be restricted until the Academy/Trust has verified the accuracy of the data
- Where an individual has objected to the processing and the Academy/Trust is considering whether their legitimate grounds override those of the individual
- Where processing is unlawful and the individual opposes erasure and requests restriction instead
- Where the Academy/Trust t no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim

13.4. If the personal data in question has been disclosed to third parties, the Academy/Trust will inform them about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so.

13.5. The Academy/Trust will inform individuals when a restriction on processing has been lifted.

14. The right to data portability

14.1. Individuals have the right to obtain and reuse their personal data for their own purposes across different services.

14.2. Personal data can be easily moved, copied or transferred from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.3. The right to data portability only applies in the following cases:

- To personal data that an individual has provided to a controller
- Where the processing is based on the individual's consent or for the performance of a contract
- When processing is carried out by automated means

14.4. Personal data will be provided in a structured, commonly used and machine-readable form.

14.5. The Academy/Trust will provide the information free of charge.

14.6. Where feasible, data will be transmitted directly to another organisation at the request of the individual.

14.7. The Academy/Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.

14.8. In the event that the personal data concerns more than one individual, the Academy/Trust will consider whether providing the information would prejudice the rights of any other individual.

14.9. The Academy/Trust will respond to any requests for portability within one month.

14.10. Where the request is complex, or a number of requests have been received, the timeframe can be extended by two months, ensuring that the individual is informed of the extension and the reasoning behind it within one month of the receipt of the request.

14.11. Where no action is being taken in response to a request, the Academy/Trust will, without delay and at the latest within one month, explain to the individual the reason for this and will inform them of their right to complain to the supervisory authority and to a judicial remedy.

15. The right to object

15.1. The Academy/Trust will inform individuals of their right to object at the first point of communication, and this information will be outlined in the privacy notice and explicitly brought to the attention of the data subject, ensuring that it is presented clearly and separately from any other information.

15.2. Individuals have the right to object to the following:

- Processing based on legitimate interests or the performance of a task in the public interest
- Direct marketing
- Processing for purposes of scientific or historical research and statistics.

15.3. Where personal data is processed for the performance of a legal task or legitimate interests:

- An individual's grounds for objecting must relate to his or her particular situation.
- The Academy/Trust will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the Academy/Trust can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

15.4. Where personal data is processed for direct marketing purposes:

- The Academy/Trust will stop processing personal data for direct marketing purposes as soon as an objection is received.
- The Academy/Trust cannot refuse an individual's objection regarding data that is being processed for direct marketing purposes.

15.5. Where personal data is processed for research purposes:

- The individual must have grounds relating to their particular situation in order to exercise their right to object.
- Where the processing of personal data is necessary for the performance of a public interest task, the Academy/Trust is not required to comply with an objection to the processing of the data.

15.6. Where the processing activity is outlined above, but is carried out online, the Academy/Trust will offer a method for individuals to object online.

16. Automated decision making and profiling

16.1. Individuals have the right not to be subject to a decision when:

- It is based on automated processing, e.g. profiling.
- It produces a legal effect or a similarly significant effect on the individual.

16.2. The Academy/Trust will take steps to ensure that individuals are able to obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.

16.3. When automatically processing personal data for profiling purposes, the Academy/Trust will ensure that the appropriate safeguards are in place, including:

- Ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the predicted impact.
- Using appropriate mathematical or statistical procedures.
- Implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors.
- Securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

16.4. Automated decisions must not concern a child or be based on the processing of sensitive data, unless:

- The Academy/Trust has the explicit consent of the individual.
- The processing is necessary for reasons of substantial public interest on the basis of Union/Member State law.

17. Privacy by design and privacy impact assessments (DPIA)

17.1. The Academy/Trust will act in accordance with the UK GDPR by adopting a privacy by design approach and implementing technical and organisational measures which demonstrate how the Academy/Trust has considered and integrated data protection into processing activities.

17.2. Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with the Academy/Trust's data protection obligations and meeting individuals' expectations of privacy.

17.3. DPIAs will allow the Academy/Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to the Academy/Trust's reputation which might otherwise occur.

17.4. A DPIA will be carried out when using new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

17.5. A DPIA will be used for more than one project, where necessary.

17.6. High risk processing includes, but is not limited to, the following:

- Systematic and extensive processing activities, such as profiling
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.
- The use of CCTV.

17.7. The Academy/Trust will ensure that all DPIAs include the following information:

- A description of the processing operations and the purposes
- An assessment of the necessity and proportionality of the processing in relation to the purpose
- An outline of the risks to individuals

- The measures implemented in order to address risk.

17.8. The Trust will ensure that any use of AI-based systems, automated decision-making tools, behavioural analytics, or cloud-integrated education platforms is subject to a Data Protection Impact Assessment (DPIA) prior to procurement or implementation. This includes assessing risks relating to fairness, transparency, bias, automated profiling, and data minimisation.

17.9. Where a DPIA indicates high risk data processing, the Academy/Trust will consult the ICO to seek its opinion as to whether the processing operation complies with the UK GDPR.

18. Data breaches

18.1. The term 'personal data breach' refers to a breach of security which has led to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

18.2. The partnership will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD training.

18.3. Where a breach is likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed.

18.4. All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the Academy/Trust becoming aware of it.

18.5. The risk of the breach having a detrimental effect on the individual, and the need to notify the relevant supervisory authority, will be assessed on a case-by-case basis.

18.6. In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the Academy/Trust will notify those concerned directly.

18.7. A 'high risk' breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.

18.8. In the event that a breach is sufficiently serious, the public will be notified without undue delay.

18.9. Effective and robust breach detection, investigation and internal reporting procedures are in place at the Academy/Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

18.10. Within a breach notification, the following information will be outlined:

- The nature of the personal data breach, including the categories and approximate number of individuals and records concerned
- The name and contact details of the DPO
- An explanation of the likely consequences of the personal data breach
- A description of the proposed measures to be taken to deal with the personal data breach
- Where appropriate, a description of the measures taken to mitigate any possible adverse effects
- Failure to report a breach when required to do so may result in a fine, as well as a fine for the breach itself.

19. Data security

19.1. Confidential paper records will be kept in a locked filing cabinet, drawer or safe, with restricted access.

19.2. Confidential paper records will not be left unattended or in clear view anywhere with general access.

19.3. Digital data is coded, encrypted or password-protected, both on a local hard drive and on a network drive that is regularly backed up off-site.

19.4. Where data is saved on removable storage or a portable device, the device will be kept in a locked filing cabinet, drawer or safe when not in use. .

19.5. Removable storage devices are not permitted on school systems. A blanket block is enforced across all Windows domain devices to prevent the use of USB storage media, mobile phones, and similar devices. The only approved exceptions are controlled devices used for specific operational purposes, such as 3D printers and designated digital audio recorders for examinations. In the College environment, USB usage is controlled through Group Policy. Limited use of USB storage devices is permitted for specific curriculum requirements, such as Sports students submitting coursework to exam boards.

19.6. All authorised electronic devices used on site must be secured with appropriate access controls, including password protection, with encryption where possible, to safeguard information in the event of loss or theft.

19.7. Where technically feasible, school-managed devices are configured to support remote security controls, including the ability to block access or erase data in the event of loss or theft.

19.8. Staff and governors are not permitted to use personal laptops or computers to store or process school data locally. Authorised College staff access internal networks remotely through a controlled VPN client. This client is installed only on College-owned devices and cannot be used on personal devices.

19.9. All members of staff are provided with their own secure login and password, passwords are enforced to be secure following DFE guidance, using either complex passwords or passphrases.

19.10. Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.

19.11. Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.

19.12. When sending confidential information by fax, staff will always check that the recipient is correct before sending.

19.13. Where personal information that could be considered private or confidential is taken off the premises, either in electronic or paper format, staff will take extra care to follow the same procedures for security, e.g. keeping devices under lock and key. The person taking the information from the Academy/Trust premises accepts full responsibility for the security of the data.

19.14. Before sharing data, all staff members will ensure:

- They are allowed to share it.
- That adequate security is in place to protect it.
- Who will receive the data has been outlined in a privacy notice.

19.15. Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of the Academy/Trust containing sensitive information are supervised at all times.

19.16. The physical security of the Academy/Trust's buildings and storage systems, and access to them is continuously monitored and reviewed.

19.17. Northern Arch Learning Partnership takes its duties under the UK GDPR seriously and any unauthorised disclosure may result in disciplinary action.

19.18. The Trust Operations & Business Manager/Schools/College IT Managers are responsible for continuity and recovery and measures are in place to ensure the security of protected data.

20. Publication of information

20.1. Northern Arch Learning Partnership publishes a publication scheme on its website outlining classes of information that will be made routinely available, including:

- Policies and procedures
- Minutes of meetings
- Annual reports
- Financial information

20.2. Classes of information specified in the publication scheme are made available quickly and easily on request.

20.3. Northern Arch Learning Partnership will not publish any personal information, including photos, on its website without the permission of the affected individual.

20.4. When uploading information to the Academy/Trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site.

21. CCTV and photography

21.1. The Academy/Trust understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

21.2. School within the Trust which has CCTV will notify all pupils, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.

21.3. Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

21.4. All CCTV footage will be kept for a maximum of 60 days (schools) and 11 days (College) for security purposes; The IT Manager/Estates Manager is responsible for keeping the records secure and allowing access.

21.5. The Academy/Trust will always indicate its intentions for taking photographs of pupils and will retrieve permission before publishing them.

21.6. If the Academy/Trust wishes to use images/video footage of pupils in a publication, such as the Academy/Trust website, prospectus, or recordings of school plays, written permission will be sought for the particular usage from the parent of the pupil.

21.7. Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the UK GDPR.

22. Data Retention

22.1. Data will not be kept for longer than is necessary in accordance with the Data Retention and Destruction Policy

23. DBS Data

23.1. All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.

23.2. Any third parties who access DBS information will be made aware of the data protection legislation, as well as their responsibilities as a data handler.

24. Training

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

24.2. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the Academy/Trust's processes make it necessary.

25. Subject Access / Subject Information Requests (SAR)

25.1. Individuals have a right to make a 'subject access request' to gain access to personal information that the Academy/Trust 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
- 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

25.2. Subject access requests must be submitted using the form below and sent by post or email to the DPO. If staff receive a subject access request, they must immediately forward it to the DPO.

26. Children and Subject Access Requests

26.1. 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.

26.2. Children have the same rights as adults to access their personal data under the UK GDPR. The right of access belongs to the child; however, in practice a parent or carer may make a subject access request on the child's behalf where they have parental responsibility. When responding to such requests, the school will consider, on a case-by-case basis, whether the child is sufficiently mature to understand their rights and the implications of the request. Where a child is considered capable, the school will normally seek to deal with the child directly or obtain their consent before disclosing personal data to a parent or carer. There is no fixed age at which a child is deemed to have this level of understanding, and each case will be assessed individually, taking into account the child's best interests and the nature of the information requested.

27. Responding to subject access requests

27.1. 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
- 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.

27.2. 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

27.3. 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.

27.4. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

27.5. When we refuse a request, we will tell the individual why and tell them they have the right to complain to the ICO.

28. Other data protection rights of the individual

28.1. 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, 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, or object to the processing of it (in certain circumstances)
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of public interest
- Request a copy of agreements under which their personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress
- 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)

28.2. 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.

Northern Arch Learning Partnership
Subject Access Request Form

Completion of the SAR form is optional. Individuals may exercise their right of access in any written format. Please complete the information below and return this form by email or post to the relevant Data Protection Officer (see details in Data Protection Policy). Please allow 1 calendar month for a response, if your request is complex or numerous this may take longer as detailed in our policy.

Title:	
Forename(s):	
Surname:	
Address:	
Telephone number:	
Email:	
Full name and Date of Birth of Data Subject if you are applying on behalf of a child	

Please provide **specific** details (and any relevant dates) of the information/documents being requested and any additional information that may enable us to locate your personal data in the box below. This will ensure the process is not delayed and we do not need to seek clarification from you.

NB: In accordance with legislation UK GDPR legislation, a request that is deemed excessive may be declined.

By completing this form, you are making a request under the UK General Data Protection Regulation (UK GDPR) for information held about you (or your child) by the Academy/Trust that you are entitled to receive.

Declaration

By signing below, you confirm that you are the Data Subject named in this Subject Access Request Form or you are legally entitled to apply for this information on their behalf. You warrant that you are the individual named and will fully indemnify the Academy/Trust for all losses and expenses incurred if you are not. If applying for a child's data, we may need to request their permission before processing this request if they are aged 13 or over. The Academy/Trust cannot accept requests in respect of your personal data from anyone else, including members of your family.

Date:	Signature: