North Halifax Grammar School

Data Protection Retention & Confidentiality Policy

Approved by:	**Principal**
Date approved:	**Spring 2019**
Next review:	**Spring 2021**
Policy owner:	**Vice Principal i/c Progress and Enrichment**

1. **Aim**

1.1. The Academy aims to protect all the privacy of all personal data it holds about students, parents and staff in line with the Data Protection Act 2018 ("the Act"), the General Data Protection Regulation (GDPR) and the Employment Practices Code and the Code of Practice.

2. **Overview of Data Protection Legislation**

2.1. The aim of the data protection legislation is to ensure that those who collect or process data ("data controllers") do not use personal information in ways incompatible with the stated purpose(s) of the data collection, and that individuals ("data subjects") know or can find out:

- What personal information is being collected about them and why;
- Whether it is accurate and kept up to date;
- In what circumstances it will be provided to third parties;

2.2. This applies whether the information is held in manual or computerised (including e-mail) format.

2.3. The GDPR sets out seven principles that must be adhered to at all times:

- Personal data shall be processed fairly and lawfully and in a transparent manner in relation to the data subject;
- Personal data shall be 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;
- Personal data shall be kept to a minimum so that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- Personal data shall be accurate and where necessary, kept up to date;
- Personal data shall be 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 shall be 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;
- The data controller (The Academy) shall be responsible for, and be able to demonstrate compliance with all of the above.

2.4. The following sections of this policy set out a brief summary of the provisions of the Act and GDPR as they are likely to apply to the Academy.

3. **Data Controller**

3.1. The Academy Trust, as a corporate body, is the "data controller" as defined by the Act. It has ultimate responsibility for compliance with the Act.

3.2. The Principal of the Academy has overall responsibility for:

- The implementation of the Act and GDPR provision and Academy policy and procedures;
- Consultation with employees and their representatives with regard to putting data protection procedures in place
- Monitoring of this policy.

4. Data Protection Registration and Notification

4.1. The Academy has registered their details with the Information Commissioner.

5. Data Protection Officer

5.1 The Academy has appointed a Data Protection Officer.

6. Definition of Personal Data

6.1. The GDPR's definition of personal data is as follows:

> *'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 to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

6.2. For more information as to the definition of personal data please see the ICO's guidance on Personal Data (website: https://ico.org.uk).

7. Categories of Personal Data

7.1. Under Article 30 of the GDPR, the school has a register of personal data it holds which includes:

purposes for processing personal data;
categories of individuals;
categories of personal data;
categories of recipients of personal data;
the name of any third countries outside the EU that the data is transferred to if applicable;

7.2. Special Category - Personal data which is more sensitive in nature is referred to as Special Category data under the GDPR. This relates to processing of personal data which relates to an individual's:

race;
ethnic origin;
political opinions;
religious or philosophical beliefs;
trade union membership;
genetic data;
biometric data (where this is used for identification purposes);
health data;
sex life; or
sexual orientation

7.3. Criminal Offence Data - Personal data which relates to criminal convictions and offences have separate safeguards for processing to that of special category data.

8. Privacy Notices

8.1. The Academy has issued Privacy Notices to inform individuals about the use of their personal data. These can be found in Annex 1 or on our website.

9. Lawful Bases for Processing

9.1. There are six lawful bases for processing data under Article 6 of the GDPR. These are as follows:

1. Consent - the data subject has given consent for processing;

2. Contract - the data subject has entered into a contract for which processing is necessary;

3. Legal Obligation - processing of personal data is necessary to comply with the law;

4. Vital Interests - processing in necessary to protect the vital interests of an individual;

5. Public Task - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

6. Legitimate Interest - processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

9.2. In the main, the Academy will carry out processing under the lawful basis of 'Public Task' in the exercise of an official authority vested in the Academy under Article 6(1)(e) of the GDPR. This includes any process which is necessary for the exercise of a task we have termed our 'Statement of Public Task', which is based on the curriculum requirements of section 78 of the Education Act 2002.

9.3. Statement of Public Task: "To deliver a balanced and broadly based curriculum which - promotes the spiritual, moral, cultural, mental and physical development of students at the school and society, and prepares students for the opportunities, responsibilities and experiences of later life. This includes the academy's trips and activities; and where appropriate, counselling services".

9.4. Where the Academy processes Special Category data the legal bases used are Article 9(2)(g) of the GDPR and Schedule 1 Part 2 of the Data Protection Act 2018 in relation to statutory and government purposes, equality or opportunity of treatment and counselling.

9.5. Where a vital interest is protected the Academy will use Article 9(2)(c); and Article 9(2) (h) and (i) for the purposes of a medical diagnosis or reasons of public health.

9.6. If the Academy needs to seek consent, the Academy will obtain this under Article 6(1)(a) Consent and section 9(2)(a) Explicit Consent for Special Category Data.

9.7. The Privacy Notices provide information to the relevant data subjects as to the Academy's lawful bases for processing their personal information.

Under Article 30 of the GDPR, the academy has a detailed register of personal data it holds which details the lawful basis for processing.

10. Data Relating to Students

10.1. If consent is the legal basis for processing data, then a child aged 13 or over is deemed capable of giving informed consent. Therefore, it is acceptable for such a child and their parents to both sign the form. For Sixth Form students, the form could be adapted so that they alone sign it. However, sometimes using an alternative basis is more appropriate and provides better protection for the child.

11. **Proposed uses for data**

11.1. Data on Websites

The general form of consent does not provide consent for the publication of personal data on the Academy's website as the publication of information on a web site requires a more informed consent, particularly where the personal data involves images of children.

11.2. Photographs and Videos

a) The Information Commissioner (who is responsible for enforcing the Act) has issued specific guidance on the taking of photographs in schools. The Act is unlikely to apply in many cases where photographs are taken in schools and, where the Act does apply, the common sense approach of asking permission to take a photograph will often be enough to ensure compliance.

b) For the avoidance of doubt, images for personal uses (e.g. a parent photographing a child and friends at a sports day to be put in the family photo album or a grandparent filming a school play) are exempt from the Act.

c) Photographs taken for official academy use may be covered by the Act and students should be advised why they are being taken. In summary, it is not strictly necessary to get the consent if the use is necessary for purposes connected with legitimate interests of the Academy.

11.3. Group photographs

a) All parents give or refuse consent when joining the NHGS community. Any parent who has expressly withheld their consent for their child's photo to be used should be excluded from published photographs as far as possible. For example, if a small group of students are photographed during a science lesson and the photo is used in a school prospectus, it is unlikely to be personal data and the Act wouldn't apply. Alternatively, if photographs are taken for building passes and are likely to be stored electronically with other personal data, the Act would apply.

b) Even though most academy literature is sent to a very specific audience, the full name of any child in the photograph should not be disclosed unless specific consent has been given to make that disclosure. Instead, only very general labels, such as "a science lesson" should be used.

11.4. Individual Photos

a) Unless specific consent to do so has been obtained, the individual student should not be identified e.g. if a photograph of an individual (such as a prize winner) is to be used in a newsletter or calendar, avoid naming that student in the text or caption accompanying the photograph unless you have their consent to do so.

11.5. Academy Events

a) If pictures are being taken at an event attended by large crowds, such as a sports' day, this is regarded as a public area so the permission of everyone in the crowd shot is not needed. People in the foreground are also considered to be in a public area. However, the photographer should address those within earshot, stating where the photograph may be published and giving them the opportunity to move away. If an image of, for example, a race winner is to be used – the crowd in the background – the race winner's verbal permission should be sought and recorded using the verbal consent form. Images of students in suitable dress should only ever be used to reduce the risk of the images being disclosed inappropriately e.g. photographs of children in swimming costumes should not be used.

11.6. Press photographs

a) Occasionally, members of the press may take photographs or film footage at the academy e.g. at an academy ceremony or if the Academy is visited by a dignitary. While the press are exempt from the Act, if the Academy specifically invites the press in for a photo call, the Act applies.

b) Some parents may object to their children appearing in the media and therefore, it is the academy will obtain consent in advance.

11.7. Using exam results

a) Examination results are categorised as Personal Data and not Special Category data.

b) Entering students for examinations is processed under the lawful basis of 'Public Task', Article 6(1)(e) of the GDPR.

c) The Information Commissioner has issued significant guidance on the publication of exam results. The guidance recognises that such publication is likely to be necessary for the purposes of legitimate interests pursued by schools. However in terms of GDPR and the Act (2018) the Academy is still waiting for updated guidance.

d) Although the Information Commissioner does not think that students or their parents must give their consent to the publication of examination results, it is best practice if the Academy ensures that students and their parents are made aware that examination results may be published. It may also be necessary to explain the form in which publication will take place.

e) In a small number of cases, publication can cause distress. When informing students or their parents that examination results are published, the academy should, therefore, advise them of the right to object to publication.

11.8. Medical information

a) See "Special Category Data " section below.

12. Consent withheld by parent or student

12.1. If a student, or the student's parents, expressly refuses to give consent to a proposed capture or use of data, that data should not be obtained or used (unless to do so is impractical, and you have fully assessed the likelihood of that student suffering harm or damage as a result and have concluded that the risk is insignificant). However, the parent or students should be informed that the refusal will, regrettably, mean the student not being able to participate in the activity in question, be it a photograph, a play or other event. Parents may be less inclined to object if it will lead to a child missing out on an experience that their friends will be able to enjoy.

13. Data Relating to Staff

13.1. Within the Academy the Principal will determine who has access to information and may be advised by the Data Protection Officer.

13.2. Data relating to staff in specific contexts is detailed below. The length of time such records are retained is included in the "Data Retention" section of this policy.

14. Data from Recruitment Process

14.1. Confidential references should not be disclosed except with the permission of the provider. Confidential references are exempt from the GDPR, under Schedule 2, Part 4 Paragraph 24(a) of the Data Protection Act 2018, this includes subject access requests by the data subject.

14.2. Background checks such as Standard Disclosures and Enhanced Disclosures through the Disclosure and Barring Service must not be kept on an individual's personal file – it must be

kept separately in a locked drawer or cupboard where it can only be accessed by those authorised to see it. It must be destroyed after 6 months by a secure method (shredding, burning or pulping) and whist waiting for destruction must be kept secure i.e. not lying around in a shredding sack or bin. A note should be kept on the personal file of the date of the disclosure, its unique reference number, the nature of the employment for which it was requested and any recruitment decision taken.

14.3. In advertising for posts the Academy will include a statement in application packs setting out the purposes for which personal information may be used. (It could be a simple statement; 'Personal information provided by candidates will be kept on a secure file in the Academy and will not be released to third parties outside the Academy without the permission of the person concerned, except where there is a legal requirement to do so.')

14.4. Requests for employment references for staff who will have responsibility for handling personal data should contain a sentence to the effect that: "If X handles personal data please comment on his/her reliability." This is likely to be relevant for most staff.

15. General Staff Records

15.1. Staff records are subject to the provisions of the Act and data, including performance reviews and disciplinary warnings is confidential.

15.2. Staff wishing to see their own personal file should make an appointment with the Personnel Officer. Copies of data held on file may be taken, but original documents must not be removed. Confidential references will not be disclosed except with the permission of the provider.

15.3. The procedure for access to personnel files is set out in **Annex 2**.

16. Health Records

16.1. In relation to sickness and ill-health records, the Academy should only retain information that is necessary to establish an employee's fitness for work. The Principal has the responsibility for determining what records are necessary.

16.2. No information about any of the health records should be made available unless it is necessary to order that that employee can fulfil their managerial role e.g. Principal or staff appointed to work on HR matters by the Principal.

17. Requests for Access to Information from Data Subject

17.1. Under the GDPR individuals can make a subject access request. This can be verbally or in writing – see template in the appendix. It would be helpful to the Academy and also ensure that processing of the request is carried out without hindrance if, when making such a request that individuals make it clear that the request is a subject access request under the GDPR.

17.2. If a data subject makes a request electronically, it is likely that the information will be provided to the data subject in an electronic format, unless requested otherwise.

17.3. The GDPR requires that information is provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information should be capable of being understood by the average person or child. There is no requirement under GDPR to translate the information for the individual.

17.4. The Academy, in most cases will not charge a fee to comply with a subject access request. However, if the request is manifestly unfounded or excessive the Academy may change a 'reasonable fee' for the administrative costs of complying with the request; or if the individual requests further copies of their data following a request (basing the fee of the administrative costs of providing further copies).

17.5. The Academy has one month to comply with a subject access request. If the end date falls on a Saturday, Sunday or bank holiday then the Academy has until the next working day to respond. Data subjects should bear in mind the following:

17.5.1. The time to respond can be extended by a further two months if the request is too complex or the Academy has received a number of requests from the individual. The individual must be told within one month of receiving the request that there will be an extension and why it is necessary.

17.5.2. Whilst the Academy will endeavour to fulfil requests during the month, individuals are asked to recognise that education establishments operate very differently to most organisations in that there are periods of time where access to staff will be limited e.g. school holidays, school trips, activity week. This will also mean that access to data will be limited. Although the Academy will endeavor to produce information in a timely manner it may well be that only part of the subject access request can be fulfilled until the school is running at full staffing capacity again. In this case it may be prudent to have a conversation with the requestor to see whether only one part of the data record is needed and therefore getting a quicker response than awaiting a full subject access response.

17.5.3. It may be necessary for the Academy to ask an individual for ID to confirm their identity before responding to the request. The Academy must notify the individual that ID is required as soon as possible upon receiving the request. Once ID has been received by the Academy then that is when the period for responding to the request begins.

17.5.4. Educational Record Requests as set out in The Education (Pupil Information) (England) Regulations 2005 may be treated differently to that of a SAR request.

17.6. In cases where a child requests access to their data the Department for Education advice is to exercise caution, especially if the data may cause a child to become upset. It cites the example of a child worrying about why the school is sending the government their test results, and advises that in this situation it might be better to address the issue in lessons alongside learning with a question and answer approach. (Data protection toolkit for schools, version 1.0, August 2018, Department for Education)

17.7. In England, Wales and Northern Ireland it is not presumed that a child aged 12 years or older is of sufficient age and maturity to be able to exercise their right of access, as is the case in Scotland. An organisation needs to consider whether the child is mature enough to understand their rights. It is still the right of the child rather than anyone else such as a parent or guardian to access information held about them. However, the Academy may allow the parent or guardian to exercise the child's rights on their behalf if the child authorises it, or it is in the best interests of the child.

17.8. Where a response to a subject access request involves providing information which not only relates to the individual making the request but also another individual then the Data Protection Act 2018 requires that the other individual has consented to the disclosure or it is reasonable to comply with the request without that individual's consent.

17.9. If the Academy decides not to comply with the request then the Academy must inform the individual without undue delay and within one month of receipt of the request. The individual should be informed as to the reasons the Academy is not taking action; inform them of their right to complain to the ICO or another supervisory authority; and their ability to seek to enforce this right through a judicial remedy.

17.10. The Principal should determine who has authority to disclose data requested by parents and/or students, and all staff should be aware of the steps to be taken if a request is made. In particular, such staff should check if the information falls into an exempt category which is not required to be disclosed.

18. **Right to be Informed**

18.1. The data subject should be informed of the reasons why the data is being held and to whom it will be disclosed. This is generally done via the Privacy Notices, and at other times when collecting or before processing personal information.

19. Right to Rectification and Erasure

19.1. The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. An individual can make a request verbally or in writing. The Academy has one calendar month to respond and in certain circumstances can refuse a request for rectification.

19.2. The GDPR includes a right for individuals to have personal data erased under certain circumstances. This right is not absolute. An individual can make a request verbally or in writing. The Academy has one calendar month to respond and in certain circumstances can refuse a request.

19.3. The data subject can apply to the Court to force correction or removal of inaccurate data. It is hoped however that steps would have been taken to correct the error long before it got to this stage. In the event of a claim being made by a data subject the Chair of Governors and the Principal must be notified immediately.

20. **Right to Restrict Processing**

20.1. The GDPR includes a right for individuals to request that personal data is restricted from processing under certain circumstances. This right is not absolute. When processing is restricted the Academy is permitted to store personal data, but not use it. An individual can make a request verbally or in writing. The Academy has one calendar month to respond and in certain circumstances can refuse a request. In most cases the restriction will be temporary for a certain period of time. An individual may also request restriction in the following scenario:.

the individual requires the Academy to store personal data in order to establish, exercise or defend a legal claim; even though the Academy no longer needs the personal data of the individual.

21. **Right to Data Portability**

21.1. Under the GDPR individuals have a right to data portability. This right only applies when the lawful basis for processing is consent **or** for the performance of a contract; and the processing is carried by automated means. The lawful bases of consent and performance of a contract are not widely used in the context of the Academy's processing. However, when the right to data portability applies an individual may receive a copy of their personal data and have their personal data transmitted from one controller to another controller, dependent on it being technically feasible and there are no legitimate reasons why transmission cannot be undertaken.

22. **Right to Object**

22.1. The GDPR gives individuals the right to object to processing of their personal data in certain circumstances. Individuals have an absolute right to opt out of direct marketing, which is the communication (by whatever means) of advertising or marketing material which is directed to particular individuals.

23. Rights related to automated decision making and profiling

23.1. The GDPR gives individuals certain rights related to automated individual decision-making (making a decision solely by automated means without human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual). If in the case the Academy wishes to use automated decision making or profiling the Academy will inform individuals of this.

24. **Exemptions**

24.1. In some cases the GDPR and the Data Protection Act 2018 allow for exemptions from some of the rights and obligations under certain circumstances. These exemptions are not routine but are based on a case-by-case basis.

25. **Disclosure to Third Parties**

25.1. All staff should be aware that they should not release personal data to a third party without a lawful basis, as defined in the Academy's Article 30 documentation (a general list of third parties and purposes is available to staff) or the consent of the data subject. Some common examples of circumstances where specific consent would have to be sought are where someone asks for an employee's home address; a building society asks for earnings details for mortgage purposes; or a journalist asks for personal details of a student. There may however be occasional circumstances when outside bodies have a statutory right to such information without consent.

26. **Police Investigations**

26.1. There is an exemption under the Act that can be applied if the police need information to prevent or detect crime or catch or prosecute a suspect. However, this exemption does not cover all personal data in all circumstances. If the information is going to be used for the stated purpose and if, by not releasing it would be likely to prejudice any attempt by the police to prevent a crime or catch a suspect, then this information can be disclosed.

27. **Fraud Detection**

27.1. Data matching for fraud detection (e.g. to detect whether the employee is receiving state benefits or not) are possible. Before the Academy participates in such a scheme the staff will be consulted. New employees must then be told of this scheme, and all employees should be reminded of it periodically under arrangements made by the Principal and approved by the Governance Board.

28. **Pension and Insurance Schemes**

28.1. Information may be supplied to a third party for pensions and insurance schemes, where such information is necessary. The employees concerned must be informed about how the information will be dealt with.

29. **Required by Government or Local Authority**

29.1. Information on both students and staff is periodically required by the government or local authority. This is sensitive personal data, and the information should be kept to a minimum, and as far as possible in an anonymous form.

30. **Send Data Abroad**

30.1. Personal data must not be transferred outside the European Economic Area unless it is being transferred to a country which has a similar data protection regime in force as the UK, or the data subject expressly consents to the transfer.

31. **Security of Data**

31.1. The GDPR requires that the Academy shall implement appropriate technical and organisational measures appropriate to the risk, to ensure that personal data shall be protected against unauthorised and unlawful processing, accidental loss, destruction or damage. The Academy shall demonstrate that processing is performed in accordance with the regulation.

The implementation of technical and organisational measures to ensure a level of security appropriate to the risk, includes inter alia as appropriate:

a) the pseudonymisation and encryption of personal data
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
d) a process for regularly testing accessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.

31.2. The Principal will take necessary precautions to ensure that both electronic and manual files are secure. The Academy will ensure that appropriate steps are taken to prevent unauthorised access to computer and manual records. Personal files must be kept secure, in locked cabinets, and not left lying about where they can be seen by unauthorised third parties.

31.3. If a staff member's duty, as an employee of the Academy, involves collecting, using or storing of personal data, the staff member has a number of legal responsibilities. These responsibilities apply whether the data is held on a computer or kept as a paper-based record, and includes items such as applications for employment, personal details collected for school trips, or staff home telephone number lists, as well as standard students and staff personal files. The staff member's responsibilities include to:

a) To collect only data that is relevant and necessary for the purpose;
b) To use the data only for the purpose specified and not further processed in a manner that is incompatible with those purposes;
c) To ensure that the data is accurate and kept up to date;
d) To ensure that the data is kept securely and not disclosed to unauthorised people, and
e) To ensure that the data is not kept for longer than necessary.

31.4. No manual or electronic employees files will be taken off the premises except in an emergency, or when expressly authorised by the Principal.

31.5. The Academy's emergency plan should provide for backup computer data to be held securely off site. Paper records should be stored securely and reasonable precautions should be taken against loss or damage.

32. **Retention of Personal Data**

32.1. As stated above, a principle of the GDPR is that personal data should not be kept for longer than is necessary for the purpose for which it was obtained. Necessity will depend on the type of data and also the determination of risk, coupled with pressures of storage space in schools. It would be impossible for all records to be kept forever and therefore a pragmatic view must be taken.

32.2. However, in the event of a claim being made against the Academy, it is important that there are appropriate records to fully investigate and potentially defend any allegations made. The difficulty for schools is that students can bring a claim in their own right (rather than through their parents) once they reach the age of 18 and therefore there remains the possibility of a student bringing a claim against a school up to 6 years after they have left senior school.

32.3. As above is the case key student records be retained until the student is aged 25. What is "key" will depend on the child and whether there are any particular concerns for their development, welfare or behaviour. For example, where there are key meetings concerning a student, such as with her parents to discuss her behaviour or academic difficulties, a copy of the notes taken should be retained for the relevant period.

32.4. The table set out in **Annex 3** summarises documents that should be retained and the minimum standards that should be followed for record retention. The Principal should ensure that procedures are in place for an annual review of records held to ensure that records are not kept longer than necessary and that expired disciplinary records are removed and destroyed.

32.5. Records containing personal data should be destroyed by shredding or by some other secure method. Personal data that is processed only for research purposes in compliance with the conditions set out in the Act may be kept indefinitely.

33. **Monitoring, evaluation and review:**

33.1 The Academy will review this policy annually and assess its implementation and effectiveness. The policy will be promoted and implemented throughout the Academy.

33.2 The Principal will report on the effectiveness of the policy to the Governance Board as appropriate.

Annex 1a

North Halifax Grammar School
Privacy Notice – Student Information

We, North Halifax Grammar School, are the Data Controller for the purposes of the General Data Protection Regulation (GDPR) and Data Protection Act 2018. The purpose of this document is to inform you of how we process student data within our control.

The categories of student information that we process include:

- personal identifiers and contacts (such as name, unique pupil number, contact details and address)
- characteristics (such as ethnicity, language, and free school meal eligibility)
- safeguarding information (such as court orders and professional involvement)
- special educational needs (including the needs and ranking)
- medical and administration (such as doctors information, child health, dental health, allergies, medication and dietary requirements)
- attendance (such as sessions attended, number of absences, absence reasons and any previous schools attended)
- assessment and attainment (such as key stage 2 results, post 16 courses enrolled for and any relevant results)
- behavioural information (such as exclusions and any relevant alternative provision put in place)
- trips and activities (dietary needs, medical needs and history and in some cases for overseas trips - passport numbers, birth certificates and divorce and marriage certificates for visas)
- catering (free school meal entitlement and purchase history)
- ID Management (photographs and names for identification badges)

This list is not exhaustive, to access the current list of categories of information we process please contact Mr R Haworth (Vice Principal) at the school.

Why we collect and use pupil information

We collect and use pupil information, for the following purposes:

a) to support student learning
b) to monitor and report on student attainment progress
c) to provide appropriate pastoral care
d) to assess the quality of our services
e) to keep children safe (food allergies, or emergency contact details)
f) to meet the statutory duties placed upon us for DfE data collections
g) to facilitate academy trips and activities
h) to provide counselling services as required
i) to protect the vital interests of a child

Under the General Data Protection Regulation (GDPR), the lawful bases we rely on for processing student information are:

Legal Obligation: Article 6(1)(c) of the GDPR for any statutory *processing which is necessary for compliance with a legal obligation to which the we are subject. This relates to tasks (e) (f) and (g) and includes the following statutory guidance:*

- *Section 537A of the Education Act 1996,*
- *The Education Act 1996 S29(3)*
- *The Education (School Performance Information) (England) Regulations 2007*
- *regulations 5 and 8 School Information (England) Regulations 2008*
- *the Education (Pupil Registration) (England) (Amendment) Regulations 2013*
- *Education and Skills Act 2008*
- *DfE Keeping Children Safe in Education Guidance 2016*
- *DfE Working Together to Safeguard Children (2015)*
- *the Management of Health & Safety at Work Regulations 1999,*

- *Regulatory Reform (Fire Safety) Order 2005 England and Wales.*
- *Health and Safety at Work Act 1974*
- *the Disability Discrimination Act 1995*

'Public Task': Public interest or in the exercise of an official authority vested in us Article 6(1)(e) of the GDPR. *This relates to tasks (a) (b) (c) (g) and (h).* This includes any process which is necessary for the exercise of a task we have termed our 'Statement of *Public Task', which is based on* the curriculum requirements of section 78 of the Education Act 2002:

> *Statement of Public Task: "To deliver a balanced and broadly based curriculum which - promotes the spiritual, moral, cultural, mental and physical development of pupils at the academy and society, and prepares pupils for the opportunities, responsibilities and experiences of later life. This includes academy trips and activities; and where appropriate counselling services".*

For the purposes of the Privacy Notice, data has been grouped into the most workable set of data items groups. Grouping can provide focus but as data items are extremely detailed in the education sector a more detailed list of purposes and the relevant legal obligations can be made available to data subjects.

Vital Interests: Article 6(1)(d) of the GDPR. Where the vital interests of a child are at risk we will use Vital Interests as a lawful basis. *This relates to task (i).*

In addition, concerning any special category data we use Article 9(2)(g) of the GDPR and Schedule 1 Part 2 of the Data Protection Act 2018 in relation to statutory and government purposes, equality or opportunity of treatment and counselling. Where a vital interest is protected we will use Article 9(2)(c); and Article 9(2) (h) and (i) for the purposes of a medical diagnosis or reasons of public health.
If we need to seek consent we will obtain this under Article 6(1)(a) Consent and section 9(2)(a) Explicit Consent for Special Category Data.

How we collect student information
We collect pupil information via:

- Data Collection Sheet at the start of each academic year
- Common Transfer Form (C2F) which is a secure file containing relevant information sent to us from the child's previous school.

Student data is essential for the academy's operational use. Whilst the majority of student information you provide to us is mandatory, some of it requested on a voluntary basis. In order to comply with the data protection legislation, we will inform you at the point of collection, whether you are required to provide certain pupil information to us or if you have a choice in this.

How we store student data
We hold student data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please visit: https://www.nhgs.co.uk/storage/app/media/Our%20Academy/Policies%20-%20NEW/Data%20Protection%20and%20Confidentiality%20Policy.pdf

Who we share student information with
We routinely share student information with:

- schools that the students attend after leaving us
- our local authority
- youth support services (students aged 13+)
- the Department for Education (DfE)

We do not share information about our students with anyone without consent unless the law and our policies allow us to do so.

Youth support services - Students aged 13+
Once our students reach the age of 13, we also pass student information to our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996.
This enables them to provide services as follows:

- youth support services
- careers advisers

The information shared is limited to the child's name, address and date of birth. However, where a parent or guardian provides their consent, other information relevant to the provision of youth support services will be shared. This right is transferred to the child / pupil once they reach the age 16.
Data is securely transferred to the youth support service via Data transferred to the DfE by the secure system COLLECT.

Students aged 16+

We will also share certain information about students aged 16+ with our local authority and / or provider of youth support services as they have responsibilities in relation to the education or training of 13-19 year olds under section 507B of the Education Act 1996. This enables them to provide services as follows:

- post-16 education and training providers
- youth support services
- careers advisers

Data is securely transferred to the youth support service via Data transferred to the DfE by the secure system COLLECT.

For more information about services for young people, please visit our local authority website.

Department for Education
The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our students with the Department for Education (DfE) either directly or via our local authority for the purpose of those data collections, under:

- Section 537A of the Education Act 1998
- the Education Act 1996 S29(3)
- the Education (School Performance Information) (England) Regulations 2007
- regulations 5 and 8 of School Information (England) Regulations 2008
- regulation 5 of The Education (Information About Individual Pupils) (England) Regulations 2013.

All data is transferred securely and held by DfE under a combination of software and hardware controls, which meet the current government security policy framework.
For more information, please see 'How Government uses your data' section.

Requesting access to your personal data
Under data protection legislation, parents and students have the right to request access to information about them that we hold. To make a request for your personal information, or be given access to your child's educational record, contact:

The Data Protection Officer:
Miss E Lewis
dpo@nhgs.co.uk
Telephone: 01422 244625

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern or complaint about the way we are collecting or using your personal data, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact The Data Protection Officer:

Miss E Lewis
dpo@nhgs.co.uk
Telephone: 01422 244625

How Government uses your data

The student data that we lawfully share with the DfE through data collections:

- underpins school funding, which is calculated based upon the numbers of children and their characteristics in each school.
- informs 'short term' education policy monitoring and school accountability and intervention (for example, school GCSE results or Pupil Progress measures).
- supports 'longer term' research and monitoring of educational policy (for example how certain subject choices go on to affect education or earnings beyond school)

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education (for example; via the school census) go to https://www.gov.uk/education/data-collection-and-censuses-for-schools

The National Pupil Database (NPD)

Much of the data about students in England goes on to be held in the National Pupil Database (NPD). The NPD is owned and managed by the Department for Education and contains information about students in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the Department.
It is held in electronic format for statistical purposes. This information is securely collected from a range of sources including schools, local authorities and awarding bodies.
To find out more about the NPD, go to https://www.gov.uk/government/publications/national-pupil-database-user-guide-and-supporting-information

Sharing by the Department

The law allows the Department to share students' personal data with certain third parties, including:

- schools
- local authorities
- researchers
- organisations connected with promoting the education or wellbeing of children in England
- other government departments and agencies
- organisations fighting or identifying crime

For more information about the Department's NPD data sharing process, please visit:
https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

Organisations fighting or identifying crime may use their legal powers to contact DfE to request access to individual level information relevant to detecting that crime. Whilst numbers fluctuate slightly over time, DfE typically supplies data on around 600 students per year to the Home Office and roughly 1 per year to the Police.

For information about which organisations the Department has provided pupil information, (and for which project) or to access a monthly breakdown of data share volumes with Home Office and the Police please visit the following website: https://www.gov.uk/government/publications/dfe-external-data-shares
To contact DfE: https://www.gov.uk/contact-dfe

Annex 1b

North Halifax Grammar School
Privacy Notice – Workforce Information

We, North Halifax Grammar School, are the Data Controller for the purposes of the General Data Protection Regulation (GDPR) and Data Protection Act 2018. The purpose of this document is to inform you of how we process workforce data within our control.

The categories of workforce information that we process include:

- personal information (such as name, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- result of Disclosure and Barring Service (DBS) check
- contact information (such as address, telephone number, email address, emergency contact details)
- pecuniary interests outside of academy (which are deemed a conflict of interest)
- medical information (such as medical needs, doctors information, GP statement of fitness to work.)
- payroll (such as bank details, salary scale, wage, deduction of earnings, pension, tax and National Insurance)
- trips and activities (dietary needs, medical needs and history and in some cases for overseas trips - passport numbers, birth certificates and divorce and marriage certificates for visas)
- ID Management (photographs and names for identification badges)
- documentation as proof of your Right to Work in the UK

This list is not exhaustive, to access the current list of categories of information we process please contact Mr R Haworth (Vice Principal) at the academy.

Why we collect and use workforce information

We collect and use workforce information, for the following purposes:

a) enable the development of a comprehensive picture of the workforce and how it is deployed
b) inform the development of recruitment and retention policies
c) enable individuals to be paid
d) to keep children safe
e) to meet the statutory duties placed upon us.
f) to facilitate school trips and activities
g) to protect the vital interests of an employee

Under the General Data Protection Regulation (GDPR), the legal basis / bases we rely on for processing personal information for general purposes are:
Legal Obligation: Article 6(1)(c) of the GDPR for any statutory *processing which is necessary for compliance with a legal obligation to which the we are subject. This relates to tasks (c) (d) and (e) and includes the following statutory guidance:*

- *Section 537A of the Education Act 1996,*
- *The Education Act 1996 S29(3)*
- *The Education (School Performance Information) (England) Regulations 2007*
- *regulations 5 and 8 School Information (England) Regulations 2008*
- *the Education (Pupil Registration) (England) (Amendment) Regulations 2013*
- *Education and Skills Act 2008*
- *DfE Keeping Children Safe in Education Guidance 2016*
- *DfE Working Together to Safeguard Children (2015)*
- *the Management of Health & Safety at Work Regulations 1999,*

- *Regulatory Reform (Fire Safety) Order 2005 England and Wales.*
- *Health and Safety at Work Act 1974*
- *the Disability Discrimination Act 1995*
- *Immigration, Asylum and Nationality Act 2006*
- *Employment Rights Act 1996*
- *Employment Relations Act 2004*
- *The Race Relations Act, 1976*

We may process workforce personal data in accordance with a 'Public Task': Public interest or in the exercise of an official authority vested in us Article 6(1)(e) of the GDPR. This relates to task (f) and includes any process which is for necessary for the exercise of a task we have termed our 'Statement of Public Task', which is based on The curriculum requirements of section 78 of the Education Act 2002:

> Statement of Public Task: *"To deliver a balanced and broadly based curriculum which - promotes the spiritual, moral, cultural, mental and physical development of students at the academy and society, and prepares pupils for the opportunities, responsibilities and experiences of later life. This includes academy trips and activities; and where appropriate counselling services".*

For the purposes of the Privacy Notice, data has been grouped into the most workable set of data items groups. Grouping can provide focus but as data items are extremely detailed in the education sector a more detailed list of purposes and the relevant legal obligations can be made available to data subjects.

Vital Interests: Article 6(1)(d) of the GDPR. Where the vital interests of an individual are at risk we will use Vital Interests as a lawful basis. This relates to task (g).

In addition, concerning any special category data we use Article 9(2)(g) of the GDPR and Schedule 1 Part 2 of the Data Protection Act 2018 in relation to statutory and government purposes, equality or opportunity of treatment and counselling. Where a vital interest is protected we will use Article 9(2)(c); and Article 9(2) (h) and (i) for the purposes of a medical diagnosis or reasons of public health.

If we need to seek consent, we will obtain this under Article 6(1)(a) Consent and section 9(2)(a) Explicit Consent for Special Category Data.

Collecting workforce information

We collect personal information via paper-based forms via the Personnel Officer.
Workforce data is essential for the school's / local authority's operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely for the set amount of time shown in our data retention schedule. For more information on our data retention schedule and how we keep your data safe, please visit our Data Protection and Confidentiality Policy via our website:
https://www.nhgs.co.uk/storage/app/media/Our%20Academy/Policies%20-%20NEW/Data%20Protection%20and%20Confidentiality%20Policy.pdf

Who we share workforce information with

We routinely share this information with:

- our local authority (where applicable)
- the Department for Education (DfE)
- EduFocus Ltd (Evolve) for school trips
- Data Plan for payroll

For Newly Qualified Teachers (NQTs) we add details to Calderdale Council's online NQT support and induction management system.

Why we share school workforce information
We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.
Local authority

We are required to share information about our workforce members with our local authority (LA) under section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education

The Department for Education (DfE) collects personal data from educational settings and local authorities via various statutory data collections. We are required to share information about our children and young people with the Department for Education (DfE) for the purpose of those data collections, under:

- Section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current **government security policy framework.**

For more information, please see 'How Government uses your data' section.
EduFocus (Ltd) Evolve
EVOLVE is an online tool for planning and managing educational visits, on-site activities, after school clubs and sports fixtures. Calderdale Council ask us to use Evolve in order to facilitate a school trip or activity, whilst ensuring any safeguarding needs are met.

Data Plan

We use Data Plan to facilitate payroll for our employees. The Data Plan GDPR Compliance policy document is available from Data Plan and available on the school network: P:\administration\GDPR - Information for staff\Privacy Notices from third companies\Dataplan GDPR Compliance Plan.

NQT Support and Induction Management System

This service allows schools to register NQTs and submit their electronic assessments securely online. The Privacy Notice for this system can be found by going to:
https://calderdale.nqtmanager.com/PrivacyPolicy.aspx?PolicyType=NQT

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact The Data Protection Officer:
Miss E Lewis
Data Protection Officer
North Halifax Grammar School
Moorbottom Road
Illingworth
HX2 9SU
Tel: 01422 244625
dpo@nhgs.co.uk

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Annex 2

Procedure for Access to Personnel Files

1. Principles

1.1 The principles that should be adopted in ensuring compliance with the Academy policy are as follows:

- All staff who have access to personnel files have a duty to maintain the confidentiality of information held on such files.
- No information held on the personnel files should be disclosed to unauthorised third parties.
- All personnel files will be securely held.

2. **Employee Access to Personnel Files**

2.1 Employees wishing to view their own personnel file must submit an advance written / email request for access to the Personnel Officer.

2.2 The Personnel Officer will provide the employee with a date and time when they are able to view their personnel file. This will be as soon as is reasonably practical but in all cases will be within 1 month of receipt of the request. Employees will be viewing their personnel file with the Personnel Officer.

2.3 No employee is allowed to remove any item appropriately stored in any personnel file.

2.4 Copies of any documents may be made if required and the Academy reserves the right to charge for this service in line with the legislation.

3. **Management Access to Personnel Files**

3.1 Personnel files of employees may be accessed by those in a management position only in the course of performing their job functions and on a need to know basis.

3.2 Managers are entitled to access the personnel files of those for whom they are managerially responsible.

3.3 Personnel files should not normally be removed but if a Manager does need to remove a file they must sign for the file and return it within 48 hours.

3.4 All files taken must be stored in a secure location.

4. **Information that will not be subject to access.**

4.1 Under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR), employees are not entitled to access information in relation to :

- Information that identifies any third party without the consent of that third party (this includes references provided to the Academy by others).
- Information of a medical nature, except where cleared by a suitable “health professional” who must confirm that the information to be disclosed does not contain anything which could cause serious physical and/or mental harm to the employee or any other person. Such material will not be disclosed to the employee without medical clearance.

5. **Incorrect information on the personnel file**

5.1 If an employee disagrees with any information that is held on their personnel file, they must immediately notify either their manager or the Principal. The employee may ask for the information to be corrected, deleted or they may write a file note disagreeing with the said item.

5.2 The final decision regarding revising, deleting or adding a file not rests with the Principal.

Annex 3

Record Retention Schedule

Type of Data	Recommended period for retention
Students	
Admission documents	Unsuccessful candidates – 1 year. Withdrawals – 1 year. Successful candidates – 6 years after the student leaves.
Coursework – Centre based	When no longer needed, the Academy can return coursework to the student, keep it or destroy it, provided any exam board appeal period has passed. If students sit exams with several exam boards, it may be administratively convenient to set a longstop date for retention of coursework by reference to the last appeal date. A sample of coursework demonstrating the range of the Year Group, plus records of marks obtained, should be retained.
Exam Scripts – External	Papers are retained by relevant exam board in accordance with their regulations. However, if a student appeals to the exam board against their final grade, they may also bring a claim against the Academy for failure to educate. Keep any relevant student data when complaints/remarks have been made throughout a student's course.
Exam Scripts – Internal	These provide useful evidence of a student's capabilities and identify difficulties. The Academy can return papers/provide copies to students to review post-exam, but are encouraged to keep original papers. Ideally, all internal papers should be kept until the student reaches 25. However, failing this, keep key stages, such as Years 7 and 9 and mocks. It may be that more material are kept in the case of problem students. A record of marks should be kept on a student's file until they are aged 25. A representative selection of de-personalised papers for each year group should also be kept, plus records of marks obtained.
Photographs	Photographs are used in school for many different purposes such as identification, educational and marketing. The different uses should be considered separately and potentially have different conditions for processing. Photographs collected and used in connection with one lawful basis should not be used for a different lawful basis. This is especially true once a student leaves. For example photographs used in the Public Task of the Academy, such as for educational purposes, should not then be used by the Academy for another lawful basis such as marketing. Once a student leaves, the Academy will have to assess whether the photograph still falls under the lawful basis for which it was collected in order to prevent any further processing. In cases where a photograph was used for marketing purposes when the individual was a student at the school; consent would need to be sought to use the photograph for marketing purposes once a student leaves. In line with this photographs should not be kept for longer than is necessary for the purpose it was processed.
Registers	Six years after a student leaves school (retention period recommended by JISC).

School Trips – Risk Assessments and General Paperwork	One year for use in future planning, unless problems were experienced, in which case retain until relevant student(s) reach age 25.
School Trips – Permission Slips	Generally, if no untoward incidents, suggest for 1 month after trip. If problems experienced, then retain until relevant student(s) reach age 25.
Summary student record (i.e. period of attendance, and other basic information).	To be retained in archive perpetuity.

Staff	
Staff records	Generally, 6 years from end of employment. See below for details of retention periods for specific documents. Note: disciplinary records must be removed in accordance with the time limits specified in the disciplinary procedures.
Written particulars of employment, contracts of employments and changes to terms and conditions	6 years from end of employment.
Application form (and other recruitment materials including notes of phone calls made/received)	6 months from end of employment (or six months from date of rejection).
References received	1 year from date received unless person employed in which case 6 years from end of employment.
References given/information to enable reference to be provided	6 years from reference/end of employment.
Induction and training records	6 years from end of employment.
Records relating to promotion, transfer, training, disciplinary Matters	6 years from end of employment.
Summary of record of services e.g. Name, position held, dates of employment	6 years from end of employment.
References provided for ex-employees	5 years.
Police Checks – DBS Disclosures	Kept for 6 months then securely destroyed. Keep date of disclosure and unique reference number.
References provided for ex-employees	5 years.
Applications for jobs – where the candidate is unsuccessful	6 months (recommended by The Discrimination Acts 1975 and 1986 and the Race Relations Act 1976).
Expense accounts	6 years.

Sickness records	3 years after the end of each tax year for Statutory Sickness Pay purposes.
Health and safety records	3 years (personal injury time limit).
Maternity records	3 years from the end of the tax year in which maternity pay period ends.
Annual leave records	2 years from the end of annual leave year, or longer if leave carried over.
Unpaid leave/special leave records	6 years from date on which made.
Annual appraisal/assessment records	6 years from end of employment.
Photographs	Photographs are used in school for many different purposes such as identification, educational and marketing. The different uses should be considered separately and potentially have different conditions for processing. Photographs collected and used in connection with one lawful basis should not be used for a different lawful basis. This is especially true once a member of staff leaves. For example photographs used in the Public Task of the Academy, such as for educational purposes, should not then be used by the Academy for another lawful basis such as marketing. Once a staff member leaves, the Academy will have to assess whether the photograph still falls under the lawful basis for which it was collected in order to prevent any further processing. In cases where a photograph was used for marketing purposes when the individual was employed at the school; consent would need to be sought to use the photograph for marketing purposes once they leaves. In line with this photographs should not be kept for longer than is necessary for the purpose it was processed.
Pension records relating to employees	12 years after benefit ceases.
Summary staff record (i.e. period of employment and other basic information, including details of unpaid absences, pension related information, and records relating to an accident or injury at work).	Until individual is aged 72.

Contact
If you would like to discuss anything in this document, then please contact:

Miss E Lewis
Data Protection Officer
North Halifax Grammar School
Moorbottom Road
Illingworth
HX2 9SU

Tel: 01422 244625

dpo@nhgs.co.uk