Data Protection Policy

Section	Contents	Page
	Statement of intent	1
1	Legal framework	1
2	Applicable data	2
3	Principles	2
4	Accountability and governance	3
5	Data protection officer (DPO)	4
6	Lawful processing	4
7	Consent	6
8	Data Protection Rights	7
9	The right to be informed	8
10	The right of access	9
11	The right to rectification	10
12	The right to erasure	10
13	The right to restrict processing	11
14	The right to data portability	11
15	The right to object	12
16	Automated decision making and profiling	13
17	Privacy by design and privacy impact assessments	14
18	Data breaches	15
19	Data security	16
20	Publication of information	17
21	CCTV	18
22	Digital and video images	18
23	Data retention	19
24	DBS data	19
25	Review	19
26	Appendices	19
	Privacy Notices	21
	Privacy Impact Assessment Template	42
	Consent Form – Digital and video images	50

Statement of intent
The Great North Wood Education Trust (The Trust) is required to keep and process certain information about its staff members and students in accordance with its legal obligations under the European Union General Data Protection Regulation (GDPR), in force from 25 May 2018. The regulation will be incorporated into United Kingdom law by the Date Protection Act 2018. This Act repeals the Data Protection Act 1998. The Trust has a statutory duty to regularly collect and share personal information about its staff or students with other organisations, in particular the Department for Education (DfE), the local authority, other government agencies and other schools. This policy is in place to ensure all staff, Trustees and governors are aware of their responsibilities and outlines how The Trust complies with the following core principles of the GDPR. This policy is not delegated to the local governing bodies as the Trust is the data controller. Organisational methods for keeping data secure are imperative, and The Trust believes that it is good practice to keep clear practical policies, backed up by written procedures

1	**Legal framework**
1.1	This policy has due regard to legislation, including, but not limited to the following: • The General Data Protection Regulation (GDPR) as enacted by the Data Protection Act 2018 • The Freedom of Information Act 2000 • The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016) • The Education (Supply of Information about the School Workforce) (No.2) (England) Regulations 2007 • The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 • The School Standards and Framework Act 1998 • The Protection of Freedoms Act 2012
1.2	This policy will also have regard to the guidance issued by the Information Commissioner's Office (ICO). Changes, arising from guidance issued by the ICO will be implemented as they arise to ensure the policy remains fully complaint.
1.3	This policy will be implemented in conjunction with the following other school policies: • Safeguarding and Child Protection Policy • ICO Good Practice on Taking Photos in School • E-security Policy • E-Communications Policy • Freedom of Information Policy • CCTV Policy • Records Management and Retention Policy.

2	**Applicable data**
2.1	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 or a unique pupil number (UPN). This policy applies to both automated personal data and to manual filing systems, where personal data is accessible according to specific criteria, as well as to chronologically ordered data and pseudonymised data, e.g. key-coded. This definition covers data transferred into other software e.g. excel, for analysis purposes and therefore the provisions of this policy apply.
2.2	Sensitive personal data is referred to 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.
2.3	Special categories of personal data in the context of this policy therefore includes: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data • Health • Sex Life • Sexual orientation.

3	**Principles**
3.1	The GDPR is based on 6 data processing principals which the Trust must follow in collecting and processing data. The Trust, as data controller, must demonstrate compliance with these principles: • Processed fairly, lawfully and in a transparent manner • Collected for specified, explicit and legitimate purposes and only further processed for reasons compatible with the purpose of collection. 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 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. Such retention is subject to implementation of the appropriate measures in order to safeguard the rights and freedoms of individuals and to meet the principal below • Processed in a manner that ensures appropriate security of the data.

4	**Accountability and Governance**
4.1	The Trust has audited the collection, processing and storage of date. Based on this audit it has implemented appropriate technical and organisational measures to demonstrate that data is processed in line with the principles listed above.
4.2	The Trust Board has given the oversight of risk management to the Audit Committee. The processing and security of data will form part of the risk register and be subject to review by the Audit Committee who in turn will report to the Trust Board.
4.2.1	The Trust Board does not delegate the Data Protection Policy to Local Governing Bodies, but has delegated policies that this policy cross references to them. The Truest Board will expect the local governing bodies to be able to demonstrate that these polices are kept under review and updated to ensure continued compliance with data protection legislation and regulations. Examples of these polices are listed at 1.3 above.
4.3	The Trust Board will ensure that the Trust wide Data Protection Policy is kept up to date and complaint.
4.4	The Trust will appoint a Data Protection Officer (DPO) (See Section 5) who will advise the schools and Trustees on compliance matter, oversee staff training, internal audits, reviews of HR policies and data protection impact assessments.
4.5	The Trust will provide comprehensive, clear and transparent privacy policies (see section 9, The right to be informed and appendices 26.1).
4.6	The 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.
4.7	To demonstrate the compliance with data protection principles internal records of the Trusts processing activities will be maintained and kept up to date. These will include: • 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

5	**Data protection officer (DPO)**
5.1	A DPO will be appointed in order to: • Inform and advise The Trust and its employees about their obligations to comply with data protection legislation • Monitor The Trust's compliance with the 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.
5.2	An existing employee may 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 e.g. if they are not involved in decisions regarding the collection, processing and storage of data. The Trust will consider sharing a DPO with another school or Trust. Consideration will be given to buying the service from the local authority or a suitably accredited organisation
5.3	The individual appointed as DPO will have professional experience and knowledge of data protection law, particularly that in relation to schools.
5.4	The DPO will report to the highest level of management at The Trust, which is the Chief Executive Officer. The DPO will also report directly to the Trust Board and/or Audit Committee to ensure their obligations are being met
5.5	The DPO will operate independently and will not be dismissed or penalised for performing their task.
5.6	Sufficient resources will be provided to the DPO to enable them to meet their GDPR obligations.

6	**Lawful processing**
6.1	The legal basis for processing data will be identified and documented prior to data being processed. This is set out below. Not everything will apply to the operation of the Trust.
6.2	Data will be lawfully processed under the following conditions: • The consent of the data subject has been obtained. • If 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 Trust in the performance of its tasks).
6.3	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).

6.4	The Trust will rely on the need to comply with a statutory obligation and the carrying out of a task in the public interest or in the exercise of official authority as the grounds for collecting and processing personal data. The legal basis will be set out in the privacy notices. (see appendix). The legal and official authority basis for collection and processing is as follows:
	• Statutory Framework for the Early Years Foundation Stage - 2017
	• Apprenticeships, Skills, Children and Learning Act (ASCL) 2009
	• Childcare Act 2006
	• Childcare Act 2016
	• Children and Families Act 2014
	• Children Act 1989, amended 2004
	• Childcare (Provision of Information about Young Children) (England) Regulations 2009
	• The Families Act 1989
	• The Education Act 1996
	• Special Education Needs and Disability Act 2001
	• SEND Code of Practice
	• Education Act 2002
	• The Academies Act 2010
	• Equalities Act 2010
	• The Children and Families Act 2014
	• The Education (Information About Individual Students) (England) Regulations 2013.
	• Keeping Children Safe in Education
	• Education Act 2005
	  o The Education (Supply of Information about the School Workforce) (No.2) (England) Regulations 2007
	• Education Act 2002
	  o Statutory Guidance : Keeping Children Safe in Education
	  o The Teachers' Disciplinary (England) Regulations 2012
	• Safeguarding Vulnerable Groups Act 2006
	• Public Services Pensions Act 2013
	• Superannuation Act 1972
	• Income Tax Act
	• The National Insurance Contributions Act
	• Academies Accounts Direction.

6.5	Collection and processing of data where there is no specific legal obligation will only be carried out where explicit and specific consent has been received.

7	**Consent**
7.1	The Trust will rely on the need to fulfil a statutory obligation as the lawful basis for data collection and processing and therefore consent will not be sought for data covered by legislation (See section 6.4). This reliance does not remove the obligation to demonstrate compliance with the principles of, and rights conferred by, the regulation.

7.2	Where consent to collect and process personal data is required it will be done in a positive way. It will not be inferred from silences or inactivity or pre-ticked boxes.
7.3	Consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes. Where consent is given, a record will be kept documenting how and when consent was given.
7.4	Consent can be withdrawn by an individual at any time. This right is restricted if data is being collected in pursuance of a statutory obligation.
7.5	The Trust ensures that consent mechanisms meet the standards of the 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.
7.6	Consent accepted under the DPA will be reviewed to ensure it meets the standards of the GDPR; however, acceptable consent obtained under the DPA will not be re-obtained.
7.7	A consent form for digital images and videos is include in the appendices. Consent will be sought when a student is admitted to school and will stay in place while they remain on roll. This does not remove the right of a parent/carer to withdraw that consent at any time. If a student moves from Rosendale Primary School to The Elmgreen School at secondary transfer fresh consent will be obtained as part of that process.
7.8	Where a child is under the age of 13 and the lawful basis of collection is not covered by legislation, the consent of parents 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.
7.9	The need for consent will not stop the sharing of information for the purposes of safeguarding and child protection The information is being processed either to 'perform a task in the public interest' or to meet a statutory obligation e.g. duties in legislation to protect children.

8	**The rights conferred by the GDPR**
8.1	The regulation confers 8 specific rights on individuals in relation to the collection and processing of their personal data: • Right to be Informed • Subject access • Rectification • Right to erasure • Right to restrict processing • Data portability • The right to object • Profiling.

8.2	The following sections 9 -17 elaborate on those rights and how the Trust will safeguard them

9	**The right to be informed**
9.1	Individuals have the right to be told why and what personal data is being collected, how it will used, who it might be shared with and how to object. To ensure individuals are informed The Trust will provide a privacy notice written in clear, plain language which is concise, transparent, easily accessible and free of charge. For instance, they will be published on all Trust websites.
9.2	If services are offered directly to a child, The Trust 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 an individual and not obtained directly from the individual, 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: o Withdraw consent at any time o Lodge a complaint with the ICO. • The existence of automated decision making, including profiling, how decisions are made, the significance of the process and the consequences.
9.4	Where data is obtained directly from the individual, 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. This information will be supplied at the time the data is obtained.
9.5	Where data is not obtained directly from the individual, information regarding the categories of personal data that The Trust holds, the source that the personal data originates from and whether it came from publicly accessible sources, will be provided.
9.7	In relation to data that is not obtained directly from the individual, this information will be supplied: • Within one month of having obtained the data • Before data is disclosed should disclosure another recipient be envisaged • At latest at the first communication if the data is being used to communicate with the individual.

10	**The right of access**
10.1	Individuals have the right to access their personal data. This right allows them confirm that their data is being processed and that it is being done lawfully.
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. The Trust will verify the identity of the person making the request before any information is supplied to avoid any possibility of a data breach.
10.3	All requests will be responded to without delay and at the latest, within one month of receipt. It is important to note that the month does not exclude school closure periods and the Trust will make arrangements to have an appropriate staff member available during these times however asking staff who are employed term time only to attend for work to deal with a SAR would represent an unreasonable cost to be incurred by the Trust.
10.4	A copy of the information will be supplied to the individual free of charge. The Trust may impose a 'reasonable fee' to comply with requests for further copies of the same information. All fees will be based on the administrative cost of providing the 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	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.
10.8	Where a request is manifestly unfounded or excessive, The 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 information Commissioners Office and to a judicial remedy, within one month of the refusal.
10.9	In the event that a large quantity of information is being processed about an individual, The Trust will ask the individual to specify the information the request is in relation to.
10.10	The Trust will manage the retention of records in accordance with its agreed policy. If the SAR relates to I information outside of the retention period the requested will be informed that the data has been destroyed and the date of destruction. The Trist will keep a log of disposal/destruction.

11	**The right to rectification**
11.1	The Trust through its internal processes will be pro-active in ensuring that personal data is accurate and up to date. Checks on data held will be carried out as often as is practicable. Notwithstanding that individuals are entitled to have any inaccurate or incomplete personal data rectified.
11.2	Requests for rectification will be responded to within one month; this will be extended by two months where the request for rectification is complex.
11.3	Where the personal data in question has been disclosed to third parties, The Trust will inform them of the rectification where possible.
11.4	Where appropriate, The Trust will inform the individual about the third parties that the data has been disclosed to. These details will be contained in the Privacy notice.
11.5	Where no action is being taken in response to a request for rectification, The Trust will explain the reason for this to the individual, and will inform them of their right to complain to ICO and to a judicial remedy.

12	**The right to erasure (the right to be forgotten)**
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 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	The right to erasure or to be forgotten also applies to personal data collected about children. Particular attention must be given to such requests as a child may not have been fully aware of the risks involved in agreeing to processing. This is most likely to be an issue on social networking sites and internet forums. Data held by the school for statutory purposes is unlikely to be erased before the agreed period in the Data Retention Policy and Privacy notice.
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 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 Trust's processing of personal data.
13.2	In the event that processing is restricted, The 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 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 Trust has verified the accuracy of the data • Where an individual has objected to the processing and The 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 Trust 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 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 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. It allows individuals to move, copy or transfer personal data from one IT environment to another in a safe and secure manner, without hindrance to usability.

14.2	This right is more likely to be exercised in a commercial setting such as accessing data on-line for price comparison purposes. The Trust provides no such services.
14.3	The right to data portability only applies in the following cases: • 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 e.g. CSV files.
14.5	The 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. However The Trust is not required to adopt or maintain processing systems which are technically compatible with other organisations.
14.7	In the event that the personal data concerns more than one individual, The Trust will consider whether providing the information would prejudice the rights of any other individual.
14.8	The Trust will respond to any requests for portability within one month. 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.
14.9	Where no action is being taken in response to a request, The 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 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 individual, 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 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 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 Trust will stop processing personal data for direct marketing purposes as soon as an objection is received. • The 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 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 Trust will offer a method for individuals to object online.

16	**Automated decision making and profiling**
16.1	The Trust has no plans to make use of automated decision making and profiling, however it will still inform Individuals that they 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 Trust will take steps to ensure that if automated decision making and profiling is used, 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 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 Trust has the explicit consent of the individual • The processing is necessary for reasons of substantial public interest on the basis law.

17	**Privacy by design and privacy impact assessments**
17.1	The Trust will adopt a privacy by design approach and implementing technical and organisational measures which demonstrate how The 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 Trust's data protection obligations and meeting individuals' expectations of privacy. A proforma is contained in the appendices based on guidance from the Information Commissioners Office.
17.3	DPIAs will allow The Trust to identify and resolve problems at an early stage, thus reducing associated costs and preventing damage from being caused to The 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. 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.
17.6	The 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
17.7	Where a DPIA indicates high risk data processing, The Trust will consult the ICO to seek its opinion as to whether the processing operation complies with data protection legislation.

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. Some breaches will be minor and will impact very few individuals others will be more extensive. A log of all breaches will be maintained by the Data Protection Officer on behalf of the Trust. All breaches must be reported to them.
18.2	The Chief Executive Officer will ensure that all staff members are made aware of, and understand, what constitutes a data breach as part of their CPD.
18.3	Where a breach is likely to result in a risk to the rights and freedoms of individuals, Information Commissioners Office will be informed.
18.4	All notifiable breaches will be reported to the Information Commissioners Office within 72 hours of The 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 Information Commissioners Office, will be assessed on a case-by-case basis. A serious breach that could leave individuals at risk of identity theft would be notifiable.
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 Trust will notify those concerned directly. A 'high risk. Breach means that the threshold for notifying the individual is higher than that for notifying the relevant supervisory authority.
18.7	In the event that a breach is sufficiently serious, the public will be notified without undue delay.
18.8	Effective and robust breach detection, investigation and internal reporting procedures are in place at The Trust, which facilitate decision-making in relation to whether the relevant supervisory authority or the public need to be notified.
18.9	A breach notification, will contain the following information: • 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.
18.10	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	The Trust recognises the risks inherent in collecting and processing personal data. It has put in place and will continue to develop processes and systems that mitigate that risk. The need for data security applies equally to paper and electronic records.
19.2	Through its IT and Broadband providers The Trust ensures the highest level of protection of its systems from external threat such as viruses , malware and ransomware. Robust systems are in place to detect and filter out potential threats.
19.3	Staff will be trained and advised on how to maintain data security. Failure to follow these procedures, that then results in a breach in security or the misuse of personal date, will be treated as a disciplinary offence. The seriousness of the breach will determine whether the offence is classified as misconduct or gross misconduct.
19.4	Confidential paper records will be • Kept in a locked filing cabinet, drawer or safe, with restricted access • Not left unattended or in clear view anywhere with general access.
19.5	All necessary members of staff are provided with their own secure login and password. Passwords must not be shared with other staff or students. Passwords should not be written down or placed on notes on or near the computer. In so far as the IT systems allow, users will be prompted to change their passwords. If a user believes their password has become compromised they should change it. Support is available from on-site IT staff.
19.6	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.
19.7	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.
19.8	Memory sticks will not be used to hold personal information unless they are password-protected and fully encrypted.
19.9	All electronic devices are password-protected to protect the information on the device in case of theft.
19.10	Where possible, The Trust enables electronic devices to allow the remote blocking or deletion of data in case of theft.
19.11	Staff and governors will not store personal data held by the Trust on their personal laptops or computers. Staff may log into the school, computer systems using a remote and secure log in. They must have a secure internet connection and adequate protection of their laptops/computers from viruses and potential hacking.

19.12	Emails containing sensitive or confidential information are password-protected if there are unsecure servers between the sender and the recipient.
19.13	The Trust will provide governors and trustees with an email account to ensure communication between is secure and with an appropriate audit trail.
19.14	Circular emails to parents are sent blind carbon copy (bcc), so email addresses are not disclosed to other recipients.
19.15	When sending confidential information by fax, staff will always check that the recipient is correct before sending.
19.16	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 Trust premises accepts full responsibility for the security of the data.
19.17	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.
19.18	The Trust currently makes limited use of Cloud facilities, but does rely on it for its daily off-site back up of data. Every care has been taken to ensure the providers offer secure systems and are compliant with data protection legislation.
19.19	Under no circumstances are visitors allowed access to confidential or personal information. Visitors to areas of The Trust containing sensitive information are supervised at all times.
19.20	The physical security of The Trust's buildings and storage systems, and access to them, is reviewed on an annual basis. If an increased risk in vandalism, burglary or theft is identified, extra measures to secure data storage will be put in place.
19.21	The Trust's Chief Financial Officer is responsible for continuity and recovery measures being in place to ensure the security of protected data.

20	**Publication of information**
20.1	The Trusts publication scheme is its website and those of the individual schools. The following classes of information that will be made routinely available, including: • Policies and procedures • Minutes of meetings • Annual reports • Financial information.

20.2	The Trust will not publish any personal information, including photos, on its website without the permission of the affected individual.
20.3	When uploading information to The Trust website, staff are considerate of any metadata or deletions which could be accessed in documents and images on the site. Documents are only published in pdf format.

21	**CCTV**
21.1	The Trust wished to provide a safe and secure environment for students, staff and visitors. It also wishes to ensure the safety of the physical assets required to deliver teaching and learning. For this reason a CCTV system has been installed covering the internal and external areas. The recording of images of identifiable individuals constitutes processing of personal information, so it is done in line with data protection principles.
21.2	Cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose
21.3	The Trust notifies all students, staff and visitors of the purpose for collecting CCTV images via notice boards, letters and email.
21.4	All CCTV footage will be kept for one month for security purposes. The Premises Manager is responsible for keeping the records secure and allowing access. .
21.5	CCTV footage is only reviewed where it is necessary to ensure the safety of staff and students or at the request of the police.

22	**Digital and video images**
22.1	The Trust and its schools value digital and video images as a way of recoding activities and celebrating the work of staff and students, They also form an important part of The Trust's promotional materials.
22.2	The Trust will always indicate its intentions for taking digital and video images of students and will obtain consent before publishing them. This consent will normally be taken at the point a student enrols at the school. It can be withdrawn at any time.
22.4	The Trust photographs staff members in order to produce photo ID as part of its safeguarding processes and to meet a statutory obligation.
22.5	Where electronic visitor management systems are in place that produce photo ID for visitors the sign in process will contain the facility to given positive consent to the photograph being taken.

22.7	Images captured by individuals for recreational/personal purposes, and videos made by parents for family use, are exempt from the GDPR. Video recording of school events will not be permitted where doing so would infringe copyright or the terms of a performing rights license.

23	**Data retention**
23.1	The Trust has an agreed and published policy on data retention
23.2	Data will not be kept for longer than is necessary.
23.3	Unrequired data will be deleted as soon as practicable.
23.4	Some educational records relating to former students or employees of The Trust may be kept for an extended period for legal reasons, but also to enable the provision of references or academic transcripts.
23.5	Paper documents will be shredded or pulped, and electronic memories scrubbed clean or destroyed, once the data should no longer be retained.

24	**DBS data**
24.1	All data provided by the DBS will be handled in line with data protection legislation; this includes electronic communication.
24.2	Data provided by the DBS will never be duplicated
24.3	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.

25	**Policy review**
25.1	This policy is normally to be reviewed every two years by the Chief Financial Officer and DPO who will make recommendations to the Board of Trustees for any changes based on practice, regulation or legislative change including case law. For the first year of operation the policy will be reviewed after 12 months
25.2	The workings of the policy will be subject to review by the Audit Committee as part of their risk management remit.

26	**Appendices**
	Privacy Notices
	Privacy Impact Assessment Template
	Consent Form – Digital and video images

Policy Created	December 2017
Approved by Trust Board	21 May 2018
Signature of Chair of Trustees Jeremy Baker	Signature of CEO Kate Atkins
Next Review	May 2019

Privacy Notice – Students and families

The Great North Wood Education Trust is the Data Controller for the information we collect about you. This notice explains why we have to collect information about you, what information we collect, how we use it and who we share it with. It also explains what rights you have over the information we have collected.

How we use student information

We use the student data:

- to support student learning
- to monitor and report on student progress
- to enter you for public examinations
- to provide appropriate pastoral care
- to participate in school residential visits
- to provide free school meals
- To ensure the safety of students through CCTV monitoring
- to assess the quality of our services
- to comply with the law regarding data sharing
- To allow the Education and Skills Agency to calculate the budget of the schools in the Trust

Why do we collect and use student information?

We collect and use student information primarily because we legally must do so. This is called a statutory duty. The laws and guidance we have to follow are:

- The Families Act 1989
- The Education Act 1996
- Special Education Needs and Disability Act 2001
- Education Act 2002
- The Academies Act 2010
- The Children and Families Act 2014
- The Education (Information about Individual Students) (England) Regulations 2013.
- Keeping Children Safe in Education

The categories of student information that we collect, hold and share include:

- Personal information (such as name, unique student number and address)
- Characteristics (such as ethnicity, language, nationality, country of birth and free school meal eligibility)
- Attendance information (such as sessions attended, number of absences and absence reasons)
- Details of any health issues such e.g. asthma, allergies etc.
- Details of who to contact in an emergency
- Information about parental contact
- Information about your attainment and progress at school
- Examination results
- Information about your behaviour at school
- Information about any special educational needs
- Information about your destination after you have left school e.g. to go to an apprenticeship or university

Collecting student information

Whilst the majority of student information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the General Data Protection Regulation, we will inform you whether you are required to provide certain student information to us or if you have a choice in this.

Storing student data

We hold student data for time which you attend the school and for set periods after you have left. We will not keep personal data any longer than is required to fulfil our legal obligations. This applies to paper records and as well as data held on computer systems. The Trust uses Capita SIMS as its management information system.

The length of time we keep data depends on the type of information and if they are any requirements from external bodies such as Department for Education to keep it for a set number of years. Where there are no legal time limits we follow best practice provided by the Information and Records Management Society (http://irms.org.uk).

Type of data	Retention Period	Action at end of retention period
Student Educational Records – Primary School	Kept whilst child at primary school	File will follow child to next educational setting e.g. secondary school
Student Educational Records – Secondary School	Date of birth + 25 years	Secure disposal
Child Protection Information on student file	Kept in sealed envelope. Date of	Secure disposal (shredding)

	birth = 25 years	
Child Protection Information – on separate file	Date of birth + 25 years then review. Check if LA social services has a copy	Secure disposal (shredding)
Special Education Needs files and ECHP	Date of birth + 25 years	Review and decide if necessary to keep
Statement of Special Educational Needs	Date of birth + 25 years	Secure disposal

Who do we share student information with?

We routinely share student information with:

- schools that the student's attend after leaving us
- our local authority
- Regional Schools Commissioner
- the Department for Education (DfE)
- the Education and Skills Funding Council
- Examination Boards
- National Health Service
- Public Health England
- School Nurse Service
- The Schools Caterers to ensure the accurate provision of free school meals and to meet dietary needs
- Parent Pay

Why we share student information

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

We share students' data with the Department for Education (DfE) on a statutory basis. This data sharing underpins school funding and educational attainment policy and monitoring.

We are required to share information about our students with the (DfE) under regulation 5 of The Education (Information About Individual Students) (England) Regulations 2013.

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.

Youth support services

What is different about 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

A parent / guardian can request that **only** their child's name, address and date of birth is passed to their local authority or provider of youth support services by informing us. This right is transferred to the child / student once he/she reaches the age 16.

Our 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

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

The National Student 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.

We are required by law, to provide information about our students to the DfE as part of statutory data collections such as the school census and early years' census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Students) (England) Regulations 2013.

To find out more about the student information we share with the department, for the purpose of data collections, go to https://www.gov.uk/education/data-collection-and-

censuses-for-schools.
To find out more about the NPD, go to
https://www.gov.uk/government/publications/national-student-database-user-guide-and-supporting-information.

The department may share information about our students from the NPD with third parties who promote the education or well-being of children in England by:

- conducting research or analysis
- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether DfE releases data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested: and
- the arrangements in place to store and handle the data

To be granted access to student information, organisations must comply with strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

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

For information about which organisations the department has provided student information, (and for which project), please visit the following website:
https://www.gov.uk/government/publications/national-student-database-requests-received

To contact DfE: https://www.gov.uk/contact-dfe

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

Geraldine Pusey, School Business Manager at Rosendale Primary School (gpusey@rosendale.cc)
Maxine Simpson, Office Manager at The Elmgreen School (msimpson@the-elmgreen-school.org.uk)
Or
Michael Burke - Acting Data Protection Officer (dpo@the-elmgreen-school.org.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
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern 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: Michael Burke - Acting Data Protection Officer (dpo@the-elmgreen-school.org.uk)

Privacy Notice – School Workforce

We process personal data relating to those we employ to work at, or otherwise engage to work at, The Great North Wood Education Trust. This is for employment purposes to assist in the running of the Trust, meet our obligations to keep children safe and to enable individuals to be paid. The collection of this information will benefit both national and local users.

How we use your information

We use your information to:

- improving the management of workforce data across the sector
- enabling development of a comprehensive picture of the workforce and how it is deployed
- informing the development of recruitment and retention policies
- allowing better financial modelling and planning
- enabling gender, ethnicity and disability monitoring
- supporting the work of the School Teachers' Review Body
- pay staff and ensure appropriate deductions of income tax, national insurance and pension are made and recorded

Why do we collect and use employee information?

We collect and use staff information primarily because we legally must do so. This is called a statutory duty. The laws and guidance we have to follow are:

- Education Act 2005
    - The Education (Supply of Information about the School Workforce) (No.2) (England) Regulations 2007
- Education Act 2002
    - Statutory Guidance : Keeping Children Safe in Education
    - The Teachers' Disciplinary (England) Regulations 2012
- Safeguarding Vulnerable Groups Act 2006
- Public Services Pensions Act 2013
- Superannuation Act 1972
- Income Tax Act
- The National Insurance Contributions Act
- Academies Accounts Direction

The categories of employee information that we collect, hold and share include:

This personal data includes identifiers such as

- Personal information (such as name, date of birth and address)
- National Insurance Number
- Emergency contact details
- Telephone number
- Email address
- Employment Contracts
- Remuneration details
- Qualifications
- Absence information
- Disciplinary matters
- Characteristics such as ethnicity, gender, medical conditions and/or disability etc.
- Photographs

Collecting employee information

Whilst the majority of employee information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with the Data Protection Legislation, we will inform you whether you are required to provide certain information to us or if you have a choice in this.

Storing employee data

We hold employee data for the time you are employed at a school in the Trist for set periods after you have left. We will not keep personal data any longer than is required to fulfil our legal obligations. This applies to paper records and as well as data held on computer systems. The Trust uses Capita SIMS as its management information system.

The length of time we keep data depends on the type of information and if they are any requirements from external bodies such as Department for Education or HM Revenue and Customs to keep it for a set number of years. Where there are no legal time limits we follow best practice provided by the Information and Records Management Society (http://irms.org.uk). Further information is available in the Trust's Record Management and Retention Policy.

Type of data	Retention Period	Action at end of retention period
Appointment of new staff	On personnel file Termination + 6 years	Secure disposal Deletion from SIMS and backup
Unsuccessful applicants paperwork	Date of appointment of successful candidate + 6 months	Secure disposal Deletion from computer systems and backup
Staff Personnel File	Termination + 6 years	Secure disposal Deletion from SIMS and backup

Type of data	Retention Period	Action at end of retention period
Appraisal records	Current year + 5 years	Secure disposal Deletion from computer systems and backup
Pre-employment checks	Termination + 6 years	Secure disposal
DBS Checks recorded on single central record	Termination + 1 year	Deletion from computer systems and backup
Maternity Pay Records	Current year + 3 years	Secure disposal

Who do we share employee information with?

We will not share information about you with third parties without your consent unless the law allows us to. We are required, by law, to routinely pass on some of this personal data to:

- the local authority
- the Department for Education (DfE)
- HM Revenue and Customs
- Local Government Pension Scheme
- Teachers' Pensions

We may be required from time to time provide information to other agencies based on statutory provision

- Office for National Statistics
- Immigration Service
- Public Health England
- Police
- The Courts
- Health and Safety Executive

Information requested by third parties for an employer's reference for mortgages and property rental will only be provided where your explicit consent has been provided.

Why we share employee information?

We share information with the Department of Education and other agencies of central and local government on a statutory basis.

Data collection requirements

The majority of data is collected on behalf of the DfE and the requirement for the Trust to collect this data is The Education (Supply of Information about the School Workforce) (No.2) (England) Regulations 2007 (Education Act 2005).

If you require more information about how we and/or DfE store and use your personal data please visit:

https://www.gov.uk/data-protection-how-we-collect-and-share-research-data

To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about them that we hold. To make a request for your personal information contact:

Geraldine Pusey, School Business Manager at Rosendale Primary School (gpusey@rosendale.cc)
Maxine Simpson, Office Manager at The Elmgreen School (msimpson@the-elmgreen-school.org.uk)
Or
Michael Burke - Acting Data Protection Officer (dpo@the-elmgreen-school.org.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
- claim compensation for damages caused by a breach of the Data Protection regulations

If you have a concern 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: Michael Burke - Acting Data Protection Officer (dpo@the-elmgreen-school.org.uk)

Privacy notice
Applicants to a new role

Prospective employees

Who processes your information?

As part of the school's recruitment process, certain information needs to be collected so your application can be considered. The following privacy notice informs you how the school intends to collect, use, process and store your data.

The Great North Wood Education Trust (The Trust) is the data controller, and they are responsible for any personal data that is provided to the school(s). This means that they determine the purposes for, and the manner in which, any personal data relating to any prospective staff member is to be processed. The processing is carried out in the individual school to whom you are making an application for employment.

A representative of the school can be contacted as follows:

Rosendale Primary School and Childrens Centre: Geraldine Pusey (gpusey@rosendale.cc)
The Elmgreen School: Maxine Simpson (msimpson@the-elmgreen-school.org.uk)

Michael Burke is the Acting Data Protection Officer (dpo@the-elmgreen-school.org.uk)
Their role is to oversee and monitor the school's data processing practices and can be contacted if you have any queries pertaining to how the school processes data.

Where necessary, third parties may be responsible for processing personal information. Where this is required, the school places data protection requirements on third party processors in line with their own data protection requirements, to ensure data is processed in line with prospective staff members' privacy rights.

Why do we need your information?

The Trust has the legal right and a legitimate interest to collect and process personal data relating to its prospective employees to ensure the school's safeguarding and safer recruitment protocols are upheld. We process personal data to meet the requirements set out in UK employment and childcare law, including those in relation to the following:

- Academy Funding Agreement
- Academy's legal framework

- Safeguarding Vulnerable Groups Act 2006
- The Childcare (Disqualification) Regulations 2009
- Keeping Children Safe in Education 2016 and any amendments
- Working Together to Safeguard Children 2015
- Individuals who are recruited will have their personal data processed to assist in the running of the school, and to enable individuals to be paid.

If prospective members of staff fail to provide their personal data, there may be significant consequences:

- Not being able to consider your application as we have insufficient information to carry out as assessment of your suitability for employment including the requirements of safer recruitment
- We cannot tell if you are barred from taking part in regulated activity and therefore you may be committing a criminal offence by applying for a position while such a prohibition exists
- Not providing us with ample proof of a right to work in the UK will prevent employment at name of school. Employees found to be working illegally could face prosecution by law enforcement officers.
- Not providing accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or you paying too much tax.
- Not providing the names and addresses of two referees including you most recent employer would mean we could not consider shortlisting you
- Not providing appropriate and relevant proof of identity and address to allow completion of a DBS check would lead to the withdrawal of an offer of employment

For which purposes are your personal data processed?

In accordance with the above, personal data pertaining to prospective members of staff is used for the following reasons:

- Statutory requirements
- Contractual requirements
- Employment checks, e.g. right to work in the UK
- Pre-employment occupational health check
- Safeguarding
- Salary requirements
- Details of who to contact on your behalf in the event of an emergency

- Which data is collected?

The personal data the school will collect from the prospective members of staff includes the following:

- Name (and any previous names)
- Phone number
- Address
- Email address
- Medical conditions

- Work history for example, previous employers and positions
- Compensation for example, basic salary or benefits
- Education and work history including professional qualifications and skills
- References, including regulated references where necessary
- Nationality, visa, proof of right to work permit information including passport, driving licence, National Insurance numbers
- Photographs and images from recorded assessments
- Results of Pre-employment screening checks for example, occupational health, criminal records checks, DfE Barred and Sanctions List, Section 128 check and European Union disqualification list
- Characteristics such as ethnic group
- Remuneration details
- Qualifications
- Absence information
- Next of Kin
- Car registration number

The collection of personal information will benefit both the DfE and The Trust by:

Improving the management of workforce data across the sector.
Enabling the development of a comprehensive picture of the workforce and how it is deployed.
Informing the development of recruitment and retention policies.
Allowing better financial modelling and planning.
Enabling ethnicity and disability monitoring.
Supporting the work of the school teachers' review body.

Will your personal data be sought from third parties?

Personal data is only sought from the data subject. No third parties will be contacted to obtain personal data pertaining to prospective members of staff without the data subject's consent.

Prospective staff members' personal data may be obtained and processed from third parties where the law requires the school to do so, e.g. medical records from a GP. The categories of data obtained and processed from third parties include:

Where data is obtained from third parties, the personal data originates from the following sources:

- Department for Education
- Professional Referees
- Previous Employer
- Occupational Health Provider
- Teachers' Pensions
- HMRC
- Home Office

How is your information shared?
The Trust will not share your personal information with any third parties without your consent, unless the law allows us to do so.

We are required, by law, to pass on some personal information to our LA and the DfE. This information is used so that relevant pre-employment checks can be made. This information can be found on certain documentation for example your passport. Documents required to perform pre-employment checks are:

- Your passport
- Your birth certificate
- Your most recent bank statement or a utility or council tax bill
- A biometric residence permit (for non EU residents)

How long is your data retained for?

Personal data is retained in line with The Trusts Records Management and Retention Policy. Personal information may be retained for varying periods of time depending on the nature of the information; you will be informed on how long your data will be obtained by the school. Data will only be retained for as long as is necessary to fulfil the purposes for which it was processed, and will not be retained indefinitely if there is no such reason for it to be.

Once your data has served its purpose it will be disposed of in line with the procedure outlined in the school's Records Management and Retention Policy. This can be downloaded from the Trust's website www.gnwet.org.uk.

What are your rights?

As the data subject, you have specific rights to the processing of your data.

You have a legal right to:

- Request access to the personal data that The Trust holds.
- Request that your personal data is amended.
- Request that your personal data is erased.
- Request that the processing of your data is restricted.
- Request to obtain and reuse your personal data for your own purposes across different services.
- Object to your consent being obtained.
- Request that your personal data is collected using automated processing.
- Where the processing of your data is based on your explicit consent, you have the right to withdraw this consent at any time. This will not affect any personal data that has been processed prior to withdrawing consent. You can withdraw consent by contacting the Data Protection Officer by email (dpo@the-elmgreen-school.org.uk)

You also have the right to lodge a complaint with the Information Commissioners Officer (ICO) in relation to how The Great North Wood Education Trust processes your personal data. If you wish to make a complaint to the ICO, you can do so on the ICO's website or call their helpline on 0303 123 1113.

How can you find out more information?

If you require further information about how we store and use your personal data, please visit the Trust website www.gnwet.org.uk to down load a copy of our Data Protection Policy and Privacy Notices. Further information is also available on the I formation Commissioner's website https://ico.org.uk.

Declaration

I, _____, declare that I have been provided with the Great North Wood Education Trust Privacy notice in relation to data processing for employment applications and understand that:

- The Great North Wood Education Trust has a legal and legitimate interest to collect and process my personal data in order to meet statutory and contractual requirements.
- There may be significant consequences if I fail to provide the personal data the school requires.
- The school may share my data with the DfE if I am successful in my application, and subsequently the LA.
- If I am successful in my application then I understand that I will receive a separate workforce privacy notice from the school.
- The Trust will not share my data with any other third parties without my consent, unless the law requires the school to do so.
- The nature and personal categories of this data, and where the personal data originates from and where my data is obtained from third parties.
- My data is retained in line with the school's Records Management and Retention Policy.
- I have rights to the processing of my personal data.

Name of prospective staff member: _____

Signature of prospective staff member: _____

Date: _____

Please return this form with you application form.

Privacy notice
Third parties

Who processes your information?

The Great North Wood Education Trust (The Trust) is the data controller, and they are responsible for any personal data that is provided to the school(s). This means that they determine the purposes for, and the manner in which, any personal data relating to any prospective staff member is to be processed. The processing is carried out in the individual school to whom you are making an application for employment.

Michael Burke is the Acting Data Protection Officer (dpo@the-elmgreen-school.org.uk) Their role is to oversee and monitor the school's data processing practices and can be contacted if you have any queries pertaining to how the school processes data.

Where necessary, third parties may be responsible for processing any personal information you provide. Where this is required, the school places data protection requirements on third-party processors to ensure data is processed in line with your privacy rights – the school is bound to the same requirements as third parties to ensure the security of personal data.

Why do we need your information?

The Trust has the legal right and a legitimate interest to collect and process personal data relating to its prospective employees to ensure the school's safeguarding and safer recruitment protocols are upheld. We process personal data to meet the requirements set out in UK employment and childcare law, including those in relation to the following:

- Safeguarding Vulnerable Groups Act 2006
- The Childcare (Disqualification) Regulations 2009
- Keeping Children Safe in Education 2016 and any amendments
- Working Together to Safeguard Children 2015
- Individuals who are recruited will have their personal data processed to assist in the running of the school, and to enable individuals to be paid.

If third parties fail to provide their personal data, there may be significant consequences. This includes the following:

- Not being able to consider your application as we have insufficient information to carry out as assessment of your suitability for employment including the requirements of safer recruitment

- We cannot tell if you are barred from taking part in regulated activity and therefore you may be committing a criminal offence by applying for a position while such a prohibition exists
- Not providing us with ample proof of a right to work in the UK will prevent employment at name of school. Employees found to be working illegally could face prosecution by law enforcement officers.
- Not providing accurate tax codes and/or national insurance numbers could lead to issues of delayed payments or you paying too much tax.
- Not providing the names and addresses of two referees including you most recent employer would mean we could not consider shortlisting you
- Not providing appropriate and relevant proof of identity and address to allow completion of a DBS check would lead to the withdrawal of an offer of employment

For which purposes are your personal data processed?

In accordance with the above, third parties' personal data is used for the following reasons:

- Statutory requirements
- Contractual requirements
- Employment checks, e.g. right to work in the UK
- Pre-employment occupational health check
- Safeguarding
- Salary requirements

Which data is collected?

The personal data the school will collect from third parties' includes the following:

- Name of organisation
- Contact information of organisation
- Name of point-of-contact
- Contractual agreements
- Remuneration details

The collection of personal information from third parties will benefit The Trust by:

- Improving the management of third-party data.
- Enabling the development of a comprehensive picture of the third parties used and how they are deployed.
- Informing the development of contracts and retention policies.
- Allowing better internal financial modelling and planning.

Will your personal data be sought from third parties?

Third parties' personal data is only sought from the data subject. No third parties will be contacted to obtain third parties' personal data without the data subject's consent.

Personal data may be obtained and processed from other third parties where the law requires the school to do so, e.g. payment information. The categories of data obtained and processed from third parties include:

Where data is obtained from third parties, the personal data originates from the following sources:

- Department for Education
- Professional Referees
- Previous Employer
- HMRC
- Home Office

How is your information shared?

The Trust will not share your personal information with any other third parties without your consent, unless the law allows us to do so.

How long is your data retained for?

Personal data is retained in line with The Trusts Records Management and Retention Policy. Personal information may be retained for varying periods of time depending on the nature of the information; you will be informed on how long your data will be obtained by the school. Data will only be retained for as long as is necessary to fulfil the purposes for which it was processed, and will not be retained indefinitely if there is no such reason for it to be.

Once your data has served its purpose it will be disposed of in line with the procedure outlined in the school's Records Management and Retention Policy. This can be downloaded from the Trust's website www.gnwet.org.uk.

What are your rights?

As the data subject, you have specific rights to the processing of your data.

You have a legal right to:

- Request access to the personal data that The Great North Wood Education Trust holds.
- Request that your personal data is amended.
- Request that your personal data is erased.
- Request that the processing of your data is restricted.
- Request to obtain and reuse your personal data for your own purposes across different services
- Object to your consent being obtained
- Request that your personal data is collected using automated processing
- Where the processing of your data is based on your explicit consent, you have the right to withdraw this consent at any time. This will not affect any personal data that

has been processed prior to withdrawing consent. You can withdraw consent by contacting the Data Protection Officer by email.

Third parties also have the right to lodge a complaint with the ICO in relation to The Great North Wood Education Trust processes their personal data. If a third party wishes to make a complaint to the ICO, they can do so on the ICO's website or they can call their helpline on 0303 123 1113.

You also have the right to lodge a complaint with the Information Commissioners Officer (ICO) in relation to how The Great North Wood Education Trust processes your personal data. If you wish to make a complaint to the ICO, you can do so on the ICO's website or call their helpline on 0303 123 1113.

How can you find out more information?

If you require further information about how we store and use your personal data, please visit the Trust website www.gnwet.org.uk to down load a copy of our Data Protection Policy and Privacy Notices. Further information is also available on the I formation Commissioner's website https://ico.org.uk.

Declaration

I, _____, declare that I have been provided with the Great North Wood Education Trust Privacy notice in relation to data processing for third parties and understand that:

- The Great North Wood Education Trust has a legal and legitimate interest to collect and process my personal data in order to meet statutory and contractual requirements.
- There may be significant consequences if I fail to provide the personal data the school requires.
- The school may share my data with the DfE if I am successful in my application, and subsequently the LA.
- The Trust will not share my data with any other third parties without my consent, unless the law requires the school to do so.
- The nature and personal categories of this data, and where the personal data originates from and where my data is obtained from third parties.
- My data is retained in line with the school's Records Management and Retention Policy.
- I have rights to the processing of my personal data.

Name of company: _____

Name of person-of-contact _____

Signature of prospective staff member: _____

Date: _____

Privacy Impact Assessment

Primary contact for advice and guidance:

Screening questions
These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

- Will the project involve the collection of new information about individuals?
- Will the project compel individuals to provide information about themselves?
- Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?
- Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?
- Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.
- Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?
- Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.
- Will the project require you to contact individuals in ways that they may find intrusive?

Step one: Identify the need for a PIA

Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.

You may find it helpful to link to other relevant documents related to the project, for example a project proposal.

Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).

Step two: Describe the information flows

You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows. You should also say how many individuals are likely to be affected by the project.

Consultation requirements

Explain what practical steps you will take to ensure that you identify and address privacy risks. Who should be consulted internally and externally? How will you carry out the consultation? You should link this to the relevant stages of your project management process.

You can use consultation at any stage of the PIA process.

Step three: Identify the privacy and related risks

Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

This table can be used to help you identify the Data Protection related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk

Step four: Identify privacy solutions

Describe the actions you could take to reduce the risks, and any future steps which would be necessary (e.g. the production of new guidance or future security testing for systems).

Risk	Solution(s)	Result: is the risk eliminated, reduced, or accepted?	Evaluation: is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?

Step five: Sign off and record the PIA outcomes

Who has approved the privacy risks involved in the project? What solutions need to be implemented?

Risk	Approved solution	Approved by

Step six: Integrate the PIA outcomes back into the project plan

Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns that may arise in the future?

Action to be taken	Date for completion of actions	Responsibility for action

Contact point for future privacy concerns

Linking the PIA to the data protection principles

Answering these questions during the PIA process will help you to identify where there is a risk that the project will fail to comply with Data Protection or other relevant legislation, for example the Human Rights Act.

Principle 1
Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:
a) at least one of the conditions in Schedule 2 is met, and
b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Principle 2
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Principle 5
Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Principle 6
Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Principle 7
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Principle 8
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?

If you will be making transfers, how will you ensure that the data is adequately protected?

Images and videos parental consent form

The Great North Wood Education Trust use images and videos to celebrate school life and students' achievements; to promote the school on social media and on the school's website; in presentations to other education providers and for other publicity purposes in printed publications, such as the prospectus, newsletters and newspapers. We cannot do this without your consent.

Please read the form thoroughly and outline your agreement as appropriate.

Name of parent/carer:	
Name of student:	
Year:	
School	

Conditions of use and Consent

Please read the following conditions thoroughly and provide your consent as appropriate by ticking either 'Yes' or 'No' for each criteria.

- This consent form is valid from the date of signature until you child leaves the school or you withdraw your consent. A new form will be required if your child moves to another school in the Trust e.g. secondary transfer.
- The school will seek further consent if a new form of publication is proposed
- It is the responsibility of parents to inform the school, in writing to the headteacher, if consent needs to be withdrawn or amended. A new consent form will be provided for completion and signature.
- You can withdraw your consent at any time. This will not affect any images used prior to the withdrawal of the consent.
- The school will not use the personal details or full names of any student in an image or video, on our website, in our school prospectuses, on social media or any other printed publications.
- The school will not include personal emails or postal addresses, telephone or fax numbers on images or videos on our website, in our school prospectuses, on social media or any other printed publications.
- The school may use pictures of students and teachers that have been drawn by students.
- The school may use work created by students.
- The school may use group or class images or videos with general labels, e.g. 'sports day'.
- The school will only use images and videos of students who are suitably dressed, i.e. it would not be suitable to display an image of a student in swimwear.
- The school will take individual, class or year group images of your child which are available to purchase annually.
- The following organisations may use images and videos of your children:
    - South London Press
    - London Borough of Lambeth

- Education Endowment Founding
- Connected Learning Centre
- BBC

I provide consent to:	Yes	No
Using images of my child on the school website.		
Using videos of my child on the school website.		
Using images of my child on social media, including the following: Twitter Facebook Instagram		
Using videos of my child on social media, including the following: Twitter Facebook Instagram		
The local media/other organisations using images of my child to publicise school events and activities (only including the organisations outlined above).		
The local media/other organisations Using videos of my child to publicise school events and activities (only including the organisations outlined above).		
Using images of my child in marketing material, e.g. the school prospectus.		
Sharing my child's data with a school-appointed external photography company for official school images. This includes the following: Name Class Roll number		

Declaration

I, _____ (name of parent), understand:

- Why my consent is required.
- The reasons why The Great Northwood Education Trust uses images and videos of my child.
- Which other organisations may use images and videos of my child.
- The conditions under which the school uses images and videos of my child.
- I have provided my consent above as appropriate, and the school will use images and videos of my child in line with my requirements.
- Consent is given for the whole of my child's time at the school named above.
- The consent is not transferable between schools in the Trust and a request for renewal will be made at transfer.
- I will be required to re-provide consent where any circumstances change.
- I can amend or withdraw my consent at any time and must do so in writing to the headteacher.

Name of parent: _____

Signature: _____

Date: _____

If you have any questions regarding this form, please do not hesitate to contact the headteacher at the school your child attends.