THE NELSON THOMLINSON SCHOOL

DATA PROTECTION POLICY

GENERAL DATA PROTECTION REGULATION

Signed by Headmaster:

Signed by Chair of Governors:

Reviewed by Curriculum Teaching and Learning Committee: 13 February 2020
Next review: February 2021

Contents

GENERAL DATA PROTECTION REGULATION

1.0 STATEMENT OF INTENT

1.1 The Nelson Thomlinson School (NTS) is committed to protecting the rights and privacy of individuals in accordance with its legal obligations under the General Data Protection Regulation (GDPR).

1.2 NTS is required to keep and process certain information about its pupils, staff and other individuals for various purposes such as:

- To support pupil learning;
- To monitor and report on pupil progress;
- To provide appropriate pastoral care;
- To assess the quality of our services;
- To ensure we operate efficiently and effectively;
- To recruit and pay staff;
- To collect payments;
- To comply with legal obligations to funding bodies and the government;
- To enable financial modelling and planning;
- To develop a comprehensive picture of the workforce and how it is deployed.

1.3 NTS may be required to share personal information about its pupils or staff with other schools, organisations, the LA and social services, and the DfE.

1.4 This policy applies to computerised systems and manual records, where personal information is accessible by specific criteria, chronologically or as pseudonymised data, e.g. key-coded. It also applies to photographs, CCTV footage and audio and video systems.

2.0 LEGAL FRAMEWORK

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

- General Data Protection Regulation (GDPR)
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998

2.2 This policy also has regard to the following guidance:

- Information Commissioner's Office (2017) 'Overview of the General Data Protection Regulation (GDPR)'
- Information Commissioner's Office (2017) 'Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now'

3.0 ASSOCIATED POLICIES

3.1 This policy should be read in conjunction with the following policies and procedures:

- Child Protection and Safeguarding
- Freedom of Information (via the LA)
- E-Safety, including use of images (photography and video)
- Records Management Policy (draft)

4.0 DEFINITIONS

4.1 **'Personal data'** refers to any information that relates to an identifiable, living individual ('data subject'). This could include information such as names, addresses, telephone numbers, photographs, expressions of opinion about an individual, or an online identifier (for example an IP address or roll number).

4.2 **'Special categories of personal data'** refers to information which is broadly the same as 'sensitive personal data' and includes biometric data, ethnicity, religious beliefs, data concerning health matters and actual or alleged criminal activities.

4.3 **'Processing'** refers to any operation which is performed on personal data such as: collection, recording, organisation, storage, alteration, retrieval, use, disclosure, dissemination or otherwise making available, combination, restriction, erasure or destruction.

4.4 **'Data Controller'** refers to any individual or organisation who controls personal data, in this instance NTS.

4.5 **'Data Subject'** refers to an individual who is the subject of the personal data, for example:

- Employees (current and former),
- Pupils (including former pupils),
- Recruitment applicants (successful and unsuccessful),
- Agency workers (current and former),
- Casual workers (current and former),
- Contract workers (current and former),
- Volunteers (including Governors) and those on work placements.

5.0 COMPLIANCE

5.1 Compliance with this policy is the responsibility of all NTS personnel who process personal data (including governors).

5.2 Any breach of this policy will result in disciplinary procedures being invoked.

5.3 Personal information will only be shared where it is lawful to do so and the third party agrees to abide by this policy and complies with the principles of the GDPR.

5.4 This policy will be updated, as necessary, to reflect best practice in data management, security and control and to ensure compliance with any change or amendment to the GDPR and any other relevant legislation.

6.0 DATA PROTECTION PRINCIPLES

6.1 In accordance with article 5 of the GDPR, personal data will be:

a) Processed lawfully, fairly and in a transparent manner.
b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.
d) Accurate and, where necessary, kept up-to-date; ensuring that inaccurate personal data is erased or rectified without delay.
e) Kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed;
f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage.

6.2 NTS will only process personal data in accordance with individuals' rights and will comply with article 5 of the GDPR in the following ways:

a) By making all reasonable efforts to ensure that data subjects are informed of the identity of the data controller; the purpose of the processing; any disclosures to third parties that are envisaged; an indication of the period for which the data will be kept, and any other information which may be relevant.
b) By ensuring that the reason for which the personal data was originally collected is the only reason for which it is processed, unless the individual is informed of any additional processing before it takes place.
c) By not seeking to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this in mind. If any irrelevant data is given by individuals, it will be destroyed immediately.
d) By reviewing and updating personal data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate. Individuals must notify NTS if a change in circumstances means that their data needs to be updated. It is the responsibility of the school to ensure that any notification regarding a change is acted on swiftly. NTS may also contact individuals to verify certain items of data.
e) By undertaking not to retain personal data for longer than is necessary to ensure compliance with the legislation, which means that NTS will undertake a regular review of the information held. This is detailed within the Records Management Policy.
f) By disposing of any personal data in a way that protects the rights and privacy of the individual concerned.
g) By ensuring appropriate technical and organisational measures are in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

6.3 Personal data may be stored for longer periods and may be processed solely for archiving in the public interest, scientific or historical research, or statistical purposes.

7.0 ACCOUNTABILITY

7.1 The Nelson Thomlinson School is the registered Data Controller with the Information Commissioner's Office (ICO) and is responsible for controlling the use and processing the personal data it has collected.

7.2 NTS will implement technical and organisational measures to demonstrate that data is being processed in line with the principles set out in this policy. This will include:

- Providing comprehensive, clear and transparent privacy notices.
- Using data protection impact assessments (DPIA), where appropriate using tools provided by the GDPR In Schools (GDPRiS) organisation.
- Recording activities relating to higher risk processing, such as the processing of special categories of personal data.

7.3 The privacy notices explain how NTS will share personal data with third parties. This will only occur following consent from the Data Protection Officer (DPO). The sharing of personal data is generally limited to enabling the school to perform its statutory duties or in respect to a child's health, safety and welfare.

7.4 Within the GDPRiS tool, a record of processing activities will include the following:

- Name and details of the organisation
- Purpose(s) of the processing
- Description of the categories of individuals and personal data
- Retention schedules
- Categories of recipients of personal data
- Description of technical and organisational security measures
- Details of transfers to third parties, including documentation of the transfer mechanism safeguards in place

7.5 Individuals who provide personal data to NTS are responsible for ensuring that the information is accurate and up-to-date.

8.0 DATA PROTECTION OFFICER (DPO)

8.1 The DPO for NTS is Mr Andy Johnson (Head of ICT & Computing). He will:

- Inform and advise NTS personnel about their obligations under this policy (including recognising a subject access request, data security and off site use).
- Ensure everyone is aware of, and understands, what constitutes a data breach.
- Provide annual training on the contents of this policy and develop and encourage best practice in school.
- Liaise with any external data controllers engaged with NTS.

- Monitor internal compliance, including identifying processing activities and checking the recording of activities related to higher risk processing, advising and checking DPIAs (including need, methodology and any safeguards) and conducting internal audits.
- Take responsibility for continuity and recovery measures to ensure the security of personal data.
- Ensure obsolete personal data is properly erased and retain a Destruction Log as part of the Records Management Policy. This will include the document description, classification, date of destruction, method and authorisation.
- Be the point of contact with the ICO, co-operate with any requests and ensure that the NTS notification is kept accurate.
- Maintain an up-to-date knowledge of data protection law in relation to schools.

8.2 The DPO will report to SMT via a Line Management process.

9.0 LAWFUL PROCESSING

9.1 Personal data can be lawfully processed under the following conditions:

a) Consent of the individual has been obtained.
b) Compliance with a legal obligation.
c) Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
d) Performance of a contract with the individual or to take steps to enter into a contract.
e) Protecting the vital interests of an individual or another person.

9.2 Special categories of personal data can be lawfully processed under the following conditions:

a) Explicit consent of the individual, unless reliance on consent is prohibited by EU or Member State law.
b) 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.
c) Processing relates to personal data manifestly made public by the individual.
d) Carrying out obligations under employment, social security or social protection law, or a collective agreement.
e) Protecting the vital interests of an individual or another person where the individual is physically or legally incapable of giving consent.
f) The establishment, exercise or defence of legal claims, or where courts are acting in their judicial capacity.
g) 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.
h) 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.
i) Reasons of public interest in the area of public health.

j) Archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes in accordance with Article 89(1).

9.3 We collect and use workforce information for general purposes under paragraphs 9.1c and 9.2g of this policy which complies with Articles 6 and 9 of the GDPR. Under any other circumstances the legal basis for processing data will be identified and documented prior to data being processed.

10.0 CONSENT

10.1 It is not always necessary to gain consent before processing personal data (see paragraphs 9.1 and 9.2) but when it is, consent must be a positive indication.

10.2 Consent will only be accepted where it is freely given, specific, informed and an unambiguous indication of the individual's wishes (it cannot be inferred from silence, inactivity or pre-ticked boxes). Consent obtained on the basis of misleading information will not be a valid basis for processing.

10.3 Any forms used to gather personal data will make reference to the privacy notice and will indicate whether or not the individual needs to give consent for the processing.

10.4 A record will be kept documenting how and when consent was given.

10.5 If an individual does not give their consent for the processing and there is no other lawful basis on which to process the data, then NTS will ensure that the processing of that data does not take place.

10.6 Consent accepted under the previous DPA will be reviewed to ensure it meets the standards of the GDPR. However, acceptable consent obtained under the DPA **will not** be reobtained.

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

10.8 **Parental consent will be sought prior to the processing of a child's data which would require consent until the age of 13**, except where the processing is related to preventative or counselling services offered directly to a child.

10.9 Consent will be sought from the child after the age of 13 if we consider they have the competence to consent for themselves. If there is any doubt parental consent will continue to be required.

11.0 THE RIGHT TO BE INFORMED

11.1 Privacy notices regarding the processing of personal data (obtained either directly or indirectly) will be concise and written in clear, accessible language.

11.2 If services are offered directly to a child, the privacy notice for pupil data will be written in a way that the child can understand.

11.3 NTS will include the following information in its privacy notices following the ICO code of practice:

- The identity and contact details of the data controller and DPO.
- The intended purpose of, and the legal basis for, processing the data.
- The legitimate interests of the data controller or third party.
- Any recipient or categories of recipients to whom the personal data will be disclosed.
- Details of transfers to third parties and the safeguards in place.
- The retention period or criteria used to determine the retention period.
- The existence of the right to access, rectification, object, erasure and withdraw consent.
- The right to complain internally and to a supervisory authority.

11.4 Where data is obtained directly from an individual, information regarding whether the provision of personal data is part of a statutory or contractual requirement and the details of the categories of personal data, as well as any possible consequences of failing to provide the personal data, will be provided at the time of collection.

11.5 Where personal data about an individual has been obtained indirectly, information regarding the source of the data and whether it was publicly accessible will be provided. This information will be supplied:

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

12.0 THE RIGHT TO ACCESS

12.1 Individuals have the right to obtain confirmation that their personal data is being processed fairly or to submit a **subject access request** (SAR) to gain access to their personal data. In order to ensure individuals receive the correct information SARs must be made in writing and submitted to the DPO.

12.2 The DPO will verify the identity of the person making the request before any information is supplied.

12.3 All requests will be responded to within one month of receipt by the DPO.

12.4 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.

12.5 Where a fair processing request is made the information contained within the relevant privacy notice will be provided.

12.6 Where a SAR is made copies of personal data will be encrypted and supplied to the individual in a commonly used electronic format.

12.7 Where a SAR is received from a pupil, the NTS policy is that:

- It will be processed in the same way as any other SAR. The information will be given directly to the pupil, unless it is clear that the pupil does not understand the nature of the request.
- Where a pupils does not appear to understand, the nature of the request will be referred to their parents or carers.
- A SAR from parents in respect of their own child will be processed as requests made on behalf of the data subject (the child) and the information will be sent either in a sealed envelope or electronically to the requesting parent. This will be provided within 15 school days in accordance with the current Education (Pupil Information) Regulations.

12.8 In the event that a large quantity of information is being processed the individual may be requested to specify the information the request is in relation to.

12.9 Where a request is excessive or repetitive, a 'reasonable fee' will be charged. All fees will be based on the administrative cost of providing the information.

12.10 Where a request is manifestly unfounded NTS holds the right to refuse to respond to the request. The individual will be informed of this decision and the reason behind it, as well as their right to complain to the supervisory authority (ICO) and to a judicial remedy, within one month of the refusal.

13.0 THE RIGHT TO RECTIFICATION

13.1 Personal data held by NTS will be as accurate as is reasonably possible.

13.2 Individuals are entitled to have any inaccurate or incomplete personal data rectified. Where an individual informs the school of inaccurate or incomplete personal data their data record will be updated as soon as is practicable.

13.3 Where personal data has been disclosed to a third party, the school will inform them of any rectification where possible. The individual will also be informed about the third parties that the data has been disclosed to where appropriate.

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

13.5 Where no action is being taken in response to a request for rectification, NTS will explain the reason for this to the individual, and will inform them of their right to complain.

14.0 THE RIGHT TO ERASURE

14.1 Individuals have the right to request erasure of personal data. This applies where:

a) Personal data is no longer necessary for the purpose for which it was collected/processed.
b) Withdrawal of consent and no other legal ground applies.
c) The individual objects to the processing and there is no overriding legitimate interest.

d) Personal data is unlawfully processed.
e) Personal data has to be erased in order to comply with a law.
f) Personal data of a child is processed in relation to an online service.

14.2 NTS has the right to refuse a request for erasure where personal data is being processed for:
a) Exercising the right of freedom of expression and information.
b) Compliance with legal obligations or for performing tasks carried out in the public interest or in exercising the data controller's official authority.
c) Reasons of public interest in the area of public health.
d) Archiving purposes in the public interest, scientific or historical research, or statistical purposes.
e) The establishment, exercise or defence of legal claims.

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

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

14.5 Where personal data has been made public and then is requested to be erased, taking into account the available technology and the cost of implementation, all reasonable steps will be taken to inform other data controllers about the request for erasure.

15.0 THE RIGHT TO RESTRICT PROCESSING

15.1 Individuals have the right to restrict the school's processing of personal data.

15.2 In the event that processing is restricted, the school 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.

15.3 The school 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 school has verified the accuracy of the data.
- Where an individual has objected to the processing and the school 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 school no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

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

15.5 The school will inform individuals when a restriction on processing has been lifted.

16.0 THE RIGHT TO DATA PORTABILITY

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

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

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

- Where personal data has been provided by an individual to NTS.
- 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.

16.4 NTS will respond to any requests for portability within one month and will provide the personal data free of charge and in a structured and commonly used form.

16.5 Where feasible, data will be transmitted directly to another organisation at the request of the individual. NTS is not required to adopt or maintain processing systems which are technically compatible with other organisations.

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

16.7 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 receipt of the request.

16.8 Where no action is being taken in response to a request NTS will, without delay and at the latest within one month, explain the reason for this. The individual will also be informed of their right to complain to the supervisory authority and to a judicial remedy.

17.0 THE RIGHT TO OBJECT

17.1 NTS will inform individuals of their right to object at the first point of communication. This will be outlined in **privacy notices** (Appendix 1a and 1b).

17.2 Individuals have the right to object to the following:

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

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

a) An individual's grounds for objecting must relate to his or her particular situation.

b) NTS will stop processing the individual's personal data unless the processing is for the establishment, exercise or defence of legal claims, or, where the school can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

17.4 Where personal data is processed for research purposes:

a) The individual must have grounds relating to their particular situation in order to exercise their right to object.

b) Where the processing of personal data is necessary for the performance of a public interest task, NTS is not required to comply with an objection to the processing of the data.

18.0 PRIVACY BY DESIGN

18.1 NTS will act in accordance with the GDPR by adopting a 'privacy by design' approach and implementing technical and organisational measures which demonstrate how the school has considered and integrated data protection into processing activities.

18.2 Data protection impact assessments (DPIAs) will be used to identify the most effective method of complying with data protection obligations and meeting individuals' expectations of privacy. These will be stored in the GDPRiS tool.

18.3 DPIAs will allow NTS to identify and resolve problems at an early stage, thus preventing reputational damage which might otherwise occur.

18.4 All DPIAs will 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.

18.5 A DPIA will be used for new technologies or when the processing is likely to result in a high risk to the rights and freedoms of individuals.

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

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

- Systematic and extensive processing activities.
- Large scale processing of special categories of data or personal data which is in relation to criminal convictions or offences.

18.8 Where a DPIA indicates high risk data processing, NTS will consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

19.0 DATA BREACH NOTIFICATION

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

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

19.3 All notifiable breaches will be reported to the relevant supervisory authority within 72 hours of the NTS DPO becoming aware of it.

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

19.5 In the event that a breach is likely to result in a high risk to the rights and freedoms of an individual, the DPO 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.

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

19.7 Effective and robust breach detection, investigation and internal reporting procedures are in place, which will guide decision-making in relation to whether the relevant supervisory authority or the public need to be notified.

19.8 Within a breach notification (stored within the GDPRiS tool), the following information will be outlined:

- The nature of the personal data breach, including categories, 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.

19.9 Failure to report a breach when required to do so will result in a fine, as well as a fine for the breach itself.

20.0 DATA SECURITY

20.1 NTS undertakes to ensure the security of the personal data it has collected. Personal data will only be accessible to those who have a valid reason for using it.

20.2 All members of NTS are responsible for ensuring that any personal data they hold is kept secure and not disclosed to any unauthorised third party (a data security user checklist is provided for quick reference in Appendix 5).

20.3 **Physical measures**

a) Premises security measures, such as alarms, safes, deadlocks, are in place.
b) Only authorised persons are allowed in the IT office.
c) Disks, tapes and printouts are locked away securely when not in use.
d) Visitors to the school are required to sign in and out, wear identification badges and are, where appropriate, accompanied.
e) Premises security and storage systems are reviewed on a regular basis.

20.4 **Technical measures**

a) Security software is installed on school networks and electronic devices. This includes:
    - Internet filtering and firewall
    - Anti-virus
    - Email ransomware detection (from September 2018)
b) Data on the school network drives is password protected and automatically backed up. There are procedures in place to access and restore all the data held on the school network drives should this be necessary.
c) NTS electronic devices are password protected.
d) Users are given a secure user name and password to access the school networks, and any other learning platform they require access to.
e) Password rules have been implemented.
f) Users will be assigned a clearance that will determine which files are accessible to them. Protected files are not accessible to unauthorised users.
g) Removable storage devices (such as USB sticks) can be used to hold personal data under the following conditions:
    - The device **must** be checked by an IT Technician before use;
    - It **must** be password protected;
    - It **must** be stored in a secure and safe place when not in use;
    - It **must not** be accessed by other users (e.g. family members) when out of school.
    - Personal data **must** be securely deleted when no longer required.

20.5 **Organisational measures**

a) Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.
b) Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation (exercise books, subject/project folders and worksheets can be stored in classrooms).
c) Paper records containing personal data **must** be kept secure if they are taken off the school premises.
d) Users **must** sign an acceptable user policy (AUP) prior to being given access to the school network. This will be up-dated periodically.
e) Passwords **must** be alphanumeric, including one capital and one special character, and be a minimum of 8 characters long to access the school network
f) User names and passwords **must not** be shared.
g) NTS electronic devices (such as staff computers) that are used to access personal data **must** be locked even if left unattended for short periods.
h) Computer terminals, CCTV camera screens etc. that show personal data **must** be placed so that they are not visible except to authorised staff.

i) Emails **must** be encrypted if they contain personal data and are being sent outside the EU.
j) Circular emails **must** be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.
k) Visitors **must not** be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
l) Visitors to school premises containing special categories of personal data **must** be supervised at all times.
m) Personal data **must not** be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.
n) Personal data **must not** be disclosed to any unauthorised third parties.
o) Personal electronic devices **must not** be used to hold personal data belonging to NTS.
p) Personal electronic devices **must** be password protected and have up-to-date, active antivirus and anti-malware checking software before being used to access personal data belonging to NTS via:
    - A password protected removable storage device;
    - The remote desktop protocol (i.e. remote access to the school network);
q) Personal electronic devices that have been set to automatically log into the school network, or school email accounts that are lost or stolen **must** be reported to the DPO so that access to these systems can be reset.
r) If personal data is taken off NTS premises, in electronic or paper format, extra care **must** be taken to follow the same procedures for security. The person taking the personal data off the school premises **must** accept full responsibility for data security.
s) Before sharing personal data, NTS staff and Governors **must** ensure:
    - They are allowed to share it;
    - That adequate security is in place to protect it;
    - Who will receive the personal data has been outlined in a privacy notice.
t) Any personal data archived on disks **must** be kept securely in a lockable cabinet.
u) NTS staff are trained regularly in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the GDPR.

21.0 CCTV AND PHOTOGRAPHY

21.1 NTS understands that recording images of identifiable individuals constitutes as processing personal data and so is done in compliance with GDPR principles.

21.2 CCTV systems operate on school premises for the purpose of protecting school members and property.

21.3 Pupils, staff, parents and visitors are notified of the purpose of collecting CCTV images via signage around the school premises.

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

21.5 CCTV footage is kept for one month for security purposes unless it is relevant to an investigation in which case it will be kept for a maximum of six months.

21.6 NTS may occasionally use photographs/videos of pupils in a publication, such as the school website, prospectus, social media page, press release, or record a school play.

21.7 Prior to the publication of any photograph or video of pupils in the press, social media, school website and prospectus or in any other marketing or promotional materials, written consent will be sought from parents. Detailed guidance is given in the E-Safety policy.

21.8 Photographs or videos captured by other individuals for recreational or personal purposes, such as pupils taking photos on a school trip or parents taking photos at prize giving, are exempt from the GDPR.

22.0 DBS DATA

22.1 DBS information is treated as a special category of personal data under this policy.

22.2 DBS information will never be duplicated and any third parties who have lawful access to DBS information will be made aware of their GDPR responsibilities.

23.0 THE SECURE TRANSFER OF DATA

23.1 NTS is required to share personal information with the Department for Education (DfE), Education and Skills Funding Agency (ESFA), Cumbria County Council (CCC), Ofsted, schools and educational institutions, public services and other third party providers. These are outlined in the Privacy notices (Appendix 1a and 1b).

23.2 Users must not remove, copy or share any personal data with a third party without permission from the DPO.

23.3 Where personal data is required to be lawfully shared with a third party it must be securely transferred either through a portal or be sent following encryption, using approved encryption software, and be password protected.

23.4 No personal data will be transferred to a country outside the European Economic Area (EEA) without the explicit consent from the individual. Advice must be taken from the DPO.

24.0 DATA RETENTION

24.1 No data will not be kept for longer than is necessary. NTS has adopted the IRMS guidelines. Further details can be found at http://irms.org.uk/page/SchoolsToolkit

24.2 The DPO will ensure that obsolete personal data is properly erased. The length of time we hold personal data is set out in our Records Management policy.

24.3 Personal data that is not required will be deleted as soon as practicable.

24.4 Some educational records relating to former pupils or employees may be kept for an extended period for legal reasons, the provision of references or for historical archives.

25.0 DATA DISPOSAL

25.1 NTS will comply with the requirements for the safe destruction and deletion of personal data when it is no longer required.

25.2 Paper documents containing personal data will be shredded or disposed of as 'confidential waste', and appropriate contract terms will be put in place with any third parties undertaking this work.

25.3 Hard drives of redundant PCs and storage devices containing personal data will be securely wiped clean before disposal, or if that is not possible, physically destroyed.

25.4 The DPO will retain a Destruction Log of personal data that is disposed of. This will include the document description, classification, date of destruction, method and authorisation.

26.0 TRAINING AND AWARENESS

26.1 NTS users receive GDPR training on an annual basis as directed by the DPO. They are made aware of their responsibilities, as described in this policy, through:

- Induction training for new staff;
- Staff meetings/briefings/INSET;
- Day to day support and guidance.

27.0 ENQUIRIES

27.1 Any further information, questions or concerns about this policy or the security of data held by NTS should be directed to the DPO, (Mr Andy Johnson, Data Protection Officer 016973 42160) or the Headmaster.

27.2 General information about the GDPR can be obtained from the Information Commissioner's Office http://www.ico.gov.uk/.

27.3 This policy will be reviewed annually and may be supplemented by additional procedures.

Appendix 1a

The Nelson Thomlinson School

Privacy Notice (How we use pupil information)

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

- Personal information (such as name, date of birth, address, unique pupil number, medical information, family circumstances/contact details and visual images/photographs)
- 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, together with any behavioural and exclusion information)
- Assessment and exam results, and post-16 learning information
- Any special educational needs
- Destination after leaving us

Why we collect and use this information

We use the pupil data:

- to support pupil learning
- to monitor and report on pupil progress
- to provide appropriate pastoral care
- to assess the quality of our services
- to comply with the law regarding data sharing
- to support pupils in deciding what to do when they leave school

The lawful basis on which we use this information

We collect and use pupil information under section 537A of the Education Act 1996, and section 83 of the Children Act 1989. We comply with Article 6(1)(c) 'Lawfulness of processing' and Article 9(2)(b) 'Processing of special categories of personal data' of the General Data Protection Regulation 2016/679 (GDPR).

Collecting pupil information from parents/guardians

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

How long do we keep information?

We keep information for as long as we need to in order to educate and look after your child. We will keep some information after your child has left the school; for example a former pupil may need confirmation of their exam results if they lose this information.

The length of time we keep pupil records is in accordance with data protection law, and guidelines from the Department for Education (DfE).

We can keep information about pupils for a very long time or even indefinitely if we might need this for historical or research purposes. For example, photographs, or information in our prospectuses.

Who we share pupil information with

- we provide all information we hold about a pupil to a school they attend after leaving us
- in accordance with our legal obligations we share information with our local authority (Cumbria County Council) and their commissioned providers of local authority services, and the Department for Education (DfE)
- we liaise with the school nursing service and NHS
- on occasion we may need to share information with the police
- we utilise a number of external educational services to assist us in fulfilling our responsibilities and to help run the school efficiently. We may need to share information with them and have ensured they all have policies in place to meet their data protection obligations. If you wish to see a list of these third parties, please contact our Data Protection Officer at school.

Why we share pupil information

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

We share pupils' 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 pupils with our local authority (LA) and the Department for Education (DfE) under section 3 of The Education (Information About Individual Pupils) (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 for pupils aged 13-19

Once our pupils reach the age of 13, we are required to pass their information to our local authority's provider of youth support services (Inspira) 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
- post-16 education and training providers

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

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

The National Pupil Database (NPD)

The NPD is owned and managed by the Department for Education (DfE) and contains information about pupils in schools in England. It provides invaluable evidence on educational performance to inform independent research, as well as studies commissioned by the DfE. 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 pupils to the DfE as part of statutory data collections such as the school census. Some of this information is then stored in the NPD. The law that allows this is the Education (Information About Individual Pupils) (England) Regulations 2013.

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

The DfE may share information about our pupils 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 DfE has robust processes in place to ensure the confidentiality of data is maintained and there are stringent controls in place regarding access and use of the data. Decisions on whether the DfE releases data to third parties are subject to a strict approval process and are 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 pupil 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 DfE'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 pupil information to, please visit: https://www.gov.uk/government/publications/national-pupil-database-requests-received
To contact DfE: https://www.gov.uk/contact-dfe

Requesting access to your personal data

Under data protection legislation, parents and pupils have the right to request access to information about them that we hold. To make a request for your personal information, or to be given access to your child's educational record, contact Mr Andrew Johnson, Data Protection Officer, at the school.
You also have the right to:

- in certain circumstances, have inaccurate personal data rectified, erased or destroyed
- object to the processing of personal data that is likely to cause, or is causing, damage or distress
- object to decisions being taken by automated means
- 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, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Contact

If you would like to discuss anything in this privacy notice, please contact Mr Andrew Johnson, Data Protection Officer, at the school.

Appendix 1b

The Nelson Thomlinson School

Privacy Notice (How we use school workforce information)

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

- personal information (such as name, address, date of birth, telephone number, employee or teacher number, national insurance number, contact details of next of kin)
- special categories of data including characteristics information such as gender, age, ethnic group, and relevant medical information
- contract information (such as start dates, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- payroll information such as bank account details
- DBS check details
- photographic records

Why we collect and use this information

We use school workforce data to:

- enable the development of a comprehensive picture of the workforce and how it is deployed
- facilitate safe recruitment
- inform the development of recruitment and retention policies
- enable individuals to be paid
- to support our duty of care towards our staff and pupils
- support effective performance management

The lawful basis on which we process this information

We collect and process workforce information under section 114 of the Education Act 2005 and Articles 6(c), 6(e) and 9(b) of the General Data Protection Regulation 2016/679 (GDPR).

Collecting this information

Whilst the majority of information you provide to us is mandatory, some of it is provided to us on a voluntary basis. In order to comply with data protection legislation, we will inform you if you have a choice in providing certain information.

Storing this information

We hold school workforce data throughout your period of employment and for 6 years after cessation of your employment.

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

Who we share this information with

We routinely share this information with:

- our local authority (Cumbria County Council)
- the Department for Education (DfE)
- Disclosure and Barring Service

Why we share school workforce information

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

Local authority

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

Department for Education (DfE)

We share personal data with the Department for Education (DfE) on a statutory basis. This data sharing underpins workforce policy monitoring, evaluation, and links to school funding/expenditure and the assessment of educational attainment.

Data collection requirements

The DfE collects and processes personal data relating to those employed by schools and local authorities that work in state funded schools (including all maintained schools, all academies and free schools and all special schools including Pupil Referral Units and Alternative Provision). All state funded schools are required to make a census submission because it is a statutory return under sections 113 and 114 of the Education Act 2005

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to https://www.gov.uk/education/data-collection-and-censuses-for-schools.

The department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

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

The department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether DfE releases personal 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 securely store and handle the data

To be granted access to school workforce information, organisations must comply with its 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

To contact the department: 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 you that we hold. To make a request for your personal information, contact Mr Andrew Johnson, Data Protection Officer, at the school.

You also have the right to:

- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- 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, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/concerns/

Further information

If you would like to discuss anything in this privacy notice, please contact Mr Andrew Johnson, Data Protection Officer, at school.

Appendix 2

ACCESS TO PERSONAL DATA REQUEST

(Subject Assess Request – SARS)

Enquirer's Surname		Enquirer's Forenames	
Enquirer's Address			
Enquirer's Postcode			
Enquirer's Tel No.			
Are you the person who is the subject of the records you are enquiring about (i.e. the "Data Subject")?			YES / NO
If NO,			
Do you have the parental responsibility for a child who is the "Data Subject" of the records you are enquiring about?			YES / NO
If Yes,			
Name of child or children about whose personal data records you are enquiring			
Description of Concerns/Area of Concern			
Description of Information or Topic(s) Requested (In your own words)			
Additional Information			

Please despatch Reply to: (if different from enquirer's details as stated on this form)

Name
Address
Postcode

DATA SUBJECT DECLARATION

I request that the School search its records based on the information supplied above under the GDPR and provide a description of the personal data found from the information described in the details outlined above relating to me (or my child/children) being processed by the School.

I agree that the reply period will commence when I have supplied sufficient information to enable the School to perform the search.

I consent to the reply being disclosed and sent to me at my stated address (or to the Despatch Name and Address above who I have authorised to receive such information).

Signature of "Data Subject" (or Subject's Parent) _____

Name of "Data Subject" (or Subject's Parent) (PRINTED) _____

Dated _____

Appendix 3

Data Security: User Checklist

This checklist is valid from May 25th 2018. It applies to all NTS staff and Governors and refers to personal data belonging to NTS (as the data controller):

- Paper records containing personal data **must not** be left unattended or in clear view anywhere with general access.
- Paper records and removable storage devices **must** be stored in a secure and safe place that avoids physical risk, loss or electronic degradation (exercise books, subject/project folders and worksheets can be stored in classrooms).
- Paper records containing personal data **must** be kept secure if they are taken off the school premises.
- Users **must** sign an acceptable user policy (AUP) prior to being given access to the school network. This will be up-dated periodically as part of the E-Safety procedures.
- Passwords **must** be alphanumeric, including one capital and one special character, and be a minimum of 8 characters long to access the school network.
- User names and passwords **must not** be shared.
- NTS electronic devices (such as staff computers) that are used to access personal data **must** be locked even if left unattended for short periods.
- Computer terminals, CCTV camera screens etc. that show personal data **must** be placed so that they are not visible except to authorised staff.
- Emails **must** be encrypted if they contain personal data and are being sent outside the EU.
- Circular emails **must** be sent blind carbon copy (bcc) to prevent email addresses being disclosed to other recipients.
- Visitors **must not** be allowed access to personal data unless they have a legal right to do so or consent has previously been given.
- Visitors to school premises containing special categories of personal data **must** be supervised at all times.

- Personal data **must not** be given over the telephone unless you are sure of the identity of the person you are speaking to and they have the legal right to request it.

- Personal data **must not** be disclosed to any unauthorised third parties.

- Removable storage devices (such as USB sticks) can be used to hold personal data under the following conditions:
  - The device **must** be checked by an IT Technician before use;
  - It **must** be password protected;
  - It **must** be stored in a secure and safe place when not in use;
  - It **must not** be accessed by other users (e.g. family members) when out of school.

- Personal data **must** be securely deleted when no longer required.

- Personal electronic devices **must not** be used to hold personal data belonging to NTS.

- Personal electronic devices **must** be password protected and have up-to-date, active anti-virus and anti-malware checking software before being used to access personal data belonging to NTS via:
  - A password protected removable storage device;
  - The remote desktop protocol (i.e. remote access to the school network);

- Personal electronic devices that have been set to automatically log into the school network or school email accounts that are lost or stolen **must** be reported to the DPO so that access to these systems can be reset.

- If personal data is taken off NTS premises, in electronic or paper format, extra care **must** be taken to follow the same procedures for security. The person taking the personal data off the school premises **must** accept full responsibility for data security.

- Before sharing personal data, NTS staff and Governors **must** ensure:
  - They are allowed to share it;
  - That adequate security is in place to protect it;
  - Who will receive the personal data has been outlined in a privacy notice.

- Any personal data archived on disks **must** be kept securely in a lockable cabinet.

- Staff are trained in the application of this policy, their responsibilities and the importance of ensuring data security in order to comply with the GDPR.

Appendix 4

Third Party Suppliers: Letter to confirm compliance with GDPR

Dear

The Nelson Thomlinson School is preparing for the implantation of the GDPR on 25th May 2018.

As a third party supplier we need you to confirm that you have undertaken a review of your processes and procedures to comply with these new regulations. To continue with our commercial relationship we need confirmation of this and an agreement that the current contract will be amended to reflect this. Please complete the series of questions below and explain how you will comply (the text is taken directly from the GDPR).

28(3) Processing by a processor must be governed by a contract that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, categories of individuals whose data is being processed and the obligations and rights of the controller. The contract must stipulate, in particular, that the processor will:

Requirement	Confirm consent and process
28(3)(a) process only on documented instructions, including regarding international transfers(unless, subject to certain restrictions, legally required to transfer to a third country or international organisation);	
28(3)(b) ensure those processing personal data are under a confidentiality obligation (contractual or statutory);	
28(3)(c) take all measures required under the security provisions (Article 32) which includes pseudonymising and encrypting personal data as appropriate;	
28(3)(d) only use a sub-processor with the controller's consent (specific or general, although where general consent is obtained processors must notify changes to controllers, giving them an opportunity to object); flow down the same contractual obligations to sub-processors;	
28(3)(e) assist the controller in responding to requests from individuals (data subjects) exercising their rights;	
28(3)(f) assist the controller in complying with the obligations relating to security, breach notification, DPIAs and consulting with supervisory authorities (Articles 32-36);	
28(3)(g) delete or return (at the controller's choice) all personal data at the end of the agreement (unless storage is required by EU/member state law);	
28(3)(h) make available to the controller all information necessary to demonstrate compliance; allow/contribute to audits (including inspections); and inform the controller if its instructions infringe data protection law.	