Northstar
New School

Data Protection Policy

This policy was reviewed by on:	This policy was ratified/reviewed by Governors on:
Date: 2 September 2019	**Date:** 28 September 2019
By: Euan Macdonald	
Policy will be reviewed on: September 2020	**Frequency of review:** Every 1 year(s)

Note: This document uses the most current Government information and guidance at the time of writing. It may change according to Government policy.

1 Interpretation

Definitions:

Criminal Convictions Data: means personal data relating to criminal convictions and offences and includes personal data relating to criminal allegations and proceedings.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal Data specifically includes, but is not limited to, contact details, health and medical information, name, age and date of birth, bank details and financial information.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special Categories of Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data.

2 Introduction

This Data protection policy sets out how Northstar New School Limited ("we", "our", "us", "the Company") handle the Personal Data of our customers, pupils, suppliers, employees, workers and other third parties.

This Data protection policy applies to all staff, including all employees, workers, contractors, agency workers, consultants, directors, members and others (“you”, “your”, “staff”). You must

read, understand and comply with this Data protection policy when Processing Personal Data on our behalf and attend training on its requirements. This Data protection policy sets out what we expect from you for the Company to comply with applicable law. Your compliance with this Data protection policy is mandatory. Any breach of this policy may result in disciplinary action.

The General Data Protection Regulation (GDPR) sets out obligations for all organisations who process Personal Data and is implemented in the UK through the Data Protection Act 2018. We are a Data Controller, meaning that we are the organisation which determines when, why and how to process Personal Data which we collect in the course of business. We are responsible for establishing practices and policies in line with the GDPR. We are the Controller of all Personal Data relating to our staff and Personal Data used in our business for our own commercial purposes.

This Data protection policy applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, clients or supplier contacts, shareholders, website users, pupils or their families or any other Data Subject.

This policy is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation.

3 | Scope

We recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is exposed to potential fines of up to EUR20 million or 4% of total worldwide annual turnover, whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

Please contact management with any questions about the operation of this Data protection policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact management in the following circumstances:

- ➔ if you are unsure about the Processing of any Personal Data, including whether you have a lawful basis for doing so, how the data is secured, whether you require Consent and so on;
- ➔ if there has been a Personal Data Breach (see paragraph 13);
- ➔ if you need any assistance dealing with any rights invoked by a Data Subject (see paragraph 15);

4 Personal data protection principles

We adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);

- collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation);
- accurate and where necessary kept up to date (Accuracy);
- not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation);
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality);
- not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and
- made available to Data Subjects and allow Data Subjects to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5 Lawfulness, fairness, transparency

Lawfulness and fairness

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

You may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing, but ensure that we Process Personal

Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

- the Data Subject has given their Consent;
- the Processing is necessary for the performance of a contract with the Data Subject (i.e. to provide agreed services or carry out obligations set out in a contract with the Data Subject);
- to comply with our legal obligations; (i.e. to pay our staff)
- to protect the Data Subject's vital interests; (this generally only applies in life or death situations where the individual is not capable of consent)
- to pursue our legitimate interests (as long as they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of the Data Subjects). The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices.

We must ensure that we have a legal basis for Processing any Personal data we hold, and that we document the basis on which we are Processing data.

6 Consent

A Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include consent. Consent must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

The circumstances in which we process data with consent as the lawful basis are likely to be limited. However, if consent is required and the Data Subject is a child, consideration must be given as to the capacity of that child to understand and give their consent. If there is any doubt about this, the consent of a parent or relevant guardian or other personal with responsibility for the child should be obtained.

If we are Processing data on the basis that the individual concerned has given their consent, they must be easily able to withdraw their consent at any time and withdrawal must be promptly honoured. If we intend to Process Personal Data for a different purpose which was not disclosed when the Data Subject first consented, we may need to obtain further consent.

If we are processing Special Category Data or Criminal Convictions Data, there are further restrictions on processing such data and consent must be explicit, meaning it must be a clear and unambiguous statement of consent and not implied by action. In the course of our work the main Special Category data we will Process is that related to health, either of our employees for the purposes of work absence, sick pay and reasonable adjustments, or our pupils for the purposes of ensuring their wellbeing is protected and they receive appropriate care. We will usually rely on a legal basis for processing other than Consent if possible. The GDPR provides that such processing is permissible for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, for medical diagnosis, and for the provision of health or social care.

We need to evidence Consent where we are relying on this for Processing data. We must therefore keep records of all Consents so that the Company can demonstrate compliance. This should be recorded on the file of each Data Subject where applicable.

7 Transparency (notifying Data Subjects)

The GDPR requires us to provide detailed, specific information to individuals whose Personal data we hold. The information must be provided through appropriate Privacy Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that they can be easily understood.

Whenever we collect Personal Data directly from the individual themselves, including for human resources or employment purposes, we must provide them with all the information required by the GDPR through a Privacy Notice which must be presented when the person first provides the Personal Data. The Company has template Privacy Notices for new employees and pupils which should be used for this purpose.

8 Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

9 Data minimisation

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You must not Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised.

10 Accuracy

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You should ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

11 Storage limitation

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

The Company will ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires that data to be kept for a minimum time.

We must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements. Data required to be retained should be anonymised where possible. Any Personal Data which we no longer require should be removed from our systems. Electronic data should be deleted from all systems and physical data should be securely destroyed by shredding/being placed in confidential waste bins for destruction.

You should ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice.

Employees

Personal Data of staff will generally be required throughout the period of their employment or contract with the company. At the point where their employment/contract ends, the data may no longer be required.

The Company generally adopts the retention periods set out in Appendix 1 of this policy in respect of employee data.

Pupils

Personal data concerning pupils should be deleted or destroyed when their relationship with the company ends and it is no longer required, subject to any legal requirements to retain particular data.

The Company generally adopts the retention periods set out in Appendix 2 of this policy in respect of pupils' data.

The length of time data is retained may vary on a case by case basis. Where data is to be retained for longer than one year, it should be archived and stored securely.

12 Security integrity and confidentiality

Protecting Personal Data

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

We therefore require to implement and maintain appropriate safeguards to ensure the security of the Personal Data we hold. All staff are responsible for protecting the Personal Data we hold, must keep it confidential and properly implement and comply with our security measures to protect against unlawful or unauthorised Processing of Personal Data or accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Special Categories of Personal Data (particularly health and medical information) from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data. You may only transfer Personal Data to third-party service providers who the Company are satisfied have adequate measures in place to protect data. Generally, the medical professionals with whom we work are data controllers in their own right and we are satisfied that appropriate arrangements are in place. .

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it;
- Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed; and
- Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

13 Reporting a Personal Data Breach

A Personal Data Breach is any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. This may result in loss, unauthorised access to, disclosure or acquisition of Personal Data. The GDPR requires us in some circumstances to notify Personal Data Breaches to the Information Commissioner and, in certain instances, the Data Subject.

Examples of a personal data breach include the following: Sending information to the wrong recipient or wrong email address/postal address/fax number, disposing of personal data in a non-confidential manner, loss or corruption of data through hacking, viruses or malware on computer systems, accidental deletion or disposal of data, loss of data in files or on a portable

device, disclosing data to a person who is not authorised to receive it.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you believe that there has been a personal data breach, you must report it as soon as you become aware of it. You should identify, where possible, what data is affected by the breach, which individuals are affected, how and when the breach occurred and any consequences or potential consequences which have come to light. You should co-operate with any investigation which requires to be carried out and preserve all evidence relating to the potential Personal Data Breach.

A record of the breach will be made, which should include the facts around the breach, how it occurred, who was affected and what steps were taken. Any manager who is made aware of a personal data breach by a member of staff should ensure that appropriate steps are taken to record the breach.

On being notified of a breach, the Company will identify any measures which can be taken to rectify the breach or minimise potential consequences and implement these where appropriate.

The Company will determine if the breach requires to be reported to the ICO in accordance with the company's obligations under data protection legislation, and whether any affected individuals require to be informed.

Failure to report a breach could have serious consequences for the individuals whose data we hold and for the company in terms of its legal obligations. It is therefore of great importance that all staff report a potential breach of personal data. Failure to inform the company of a Personal Data Breach or deliberately taking steps to conceal a breach may result in action being taken under our Disciplinary Policy.

14 Transfer limitation

The GDPR restricts data transfers to countries outside the European Economic Area (EEA) (being the countries in the EU, and Iceland, Liechtenstein and Norway) to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

We do not envisage that Personal Data should require to be transferred outside the EEA in the usual course of our business, but if this is the case you should seek guidance before carrying out

any such transfer.

15 Data Subject's rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time;
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold;
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected, to rectify inaccurate data or to complete incomplete data;
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on automated processing, including profiling (ADM) (these being decisions made without human intervention);
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority, being the Information Commissioner.;
- in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a digital format; and

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any request you receive to exercise any of these rights to the Matron.

16 Accountability

Under the GDPR, we must be able to demonstrate, compliance with the data protection principles.

The Company must therefore have adequate resources and controls in place to ensure and to document GDPR compliance including:

- completing Data Protection Impact Assessments (DPIAs) where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this Data protection policy,;
- training Company Personnel on the GDPR, this Data protection policy, and data protection matters including, for example, Data Subject's rights, Consent, legal basis, and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and
- testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance.

17 Record keeping

The GDPR requires us to keep full and accurate records of all our data Processing activities.

These records should include, at a minimum:

- the name and contact details of the Controller and any person appointed to oversee privacy and data protection matters
- clear descriptions of the types of data held (i.e. contact details, medical information, date of birth)
- descriptions of the Data Subject types (i.e. what types of people or groups do we hold data

about) - details of the what processing we carry out and for what purposes

- details of any third-party recipients of the data we hold
- where data is stored and what security measures are in place
- how long the data is retained for
- details of any transfers of personal data

18 Training and audit

We have to ensure all Company Personnel have adequate training to enable them to comply with data privacy laws.

All staff must undergo all mandatory data privacy related training.

We must ensure that our systems and processes comply with data protection principles and adequately protect personal data. If you become aware of or consider there is an issue with any of our processes or systems which may compromise data security, you must advise management.

19 Data Protection Impact Assessment (DPIA)

If we implement any new systems or processes, we must take account of data protection requirements and any implications in respect of the proposed new system or process, and must conduct a Data Protection Impact Assessment (DPIA). We may also conduct a DPIA more generally as part of risk assessment.

A DPIA must include:

- a description of the Processing and its purposes;
- an assessment of the necessity and proportionality of the Processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

20 Sharing Personal Data

Generally we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of the Company if the recipient has a job-related need to know the information.

Third parties with whom we share personal data may include:

- Accountants, payroll processors and our pension provider in respect of employee pay and benefits;
- The General Teaching Council for England;
- Medical or other professionals in respect of pupils, including doctors, dentists, optometrists, psychologists, social workers, and so on.
- Local authorities in respect of referrals.

You may only share the Personal Data we hold with third parties, such as our service providers, if:

they have a need to know the information for the purposes of providing the contracted services;

sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

21 Changes to this Policy

We may make changes to this policy in accordance with any changes to applicable laws or guidelines or changes to the Company's practice. This policy does not override any applicable UK data privacy laws and regulations.

22 Acknowledgement of receipt and review

I, ……..…….. acknowledge that on ……., I received and read a copy of Northstar New School Limited's Data protection policy and understand that I am responsible for knowing and abiding by its terms. This Policy does not set terms or conditions of employment or form part of an employment contract.

Signed ……..

Printed Name ……..

Date ……..

Appendix 1 | Retention of employment records

Type of employment record	Retention period
Recruitment records These may include: Completed online application forms or CVs. Equal opportunities monitoring forms. Assessment exercises or tests. Notes from interviews and short-listing exercises. Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.) Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)	Six months after notifying candidates of the outcome of the recruitment exercise.
Immigration checks	Seven years after the termination of employment.
Contracts, including: Written particulars of employment. Contracts of employment or other contracts. Documented changes to terms and conditions.	While employment continues and for seven years after the contract ends.
Payroll and wage records Details on overtime. Expenses. Benefits	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.

Current bank details	Bank details will be deleted as soon after the end of employment as possible once final payments have been made
PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Personnel records including: Qualifications/references. Annual leave records. Annual assessment reports/reviews/appraisals. Disciplinary procedures. Grievance procedures. Resignation, termination and retirement details.	While employment continues and for seven years after employment ends.
Working time opt-out	Three years from the date on which they were entered into.
Records to show compliance with working time, including: Time sheets for opted-out workers. Health assessment records for night workers.	Three years after the relevant period.
Maternity/paternity records including: Maternity/paternity/shared parental payments.	Seven years after the end of the tax year in which the maternity/paternity/shared parental/adoption pay period ends.

Dates of maternity/paternity/shared parental/adoption leave. Period without maternity payment. Maternity certificates showing the expected week of confinement.	
Accident records regarding any reportable accident, death or injury in connection with work.	For at least seven years from the date the report was made.

Appendix 2 | Retention of pupil's personal data

Type of record	Retention Period
Personal details – name, date of birth	
Relative/carer/guardian contact details	
Former schools and education history	
Health/medical information including details of medical conditions and treatment, specific educational needs or adjustments required.	
Records of educational achievement, attendance, behaviour, safeguarding concerns	
Accident records	
Learning plans and arrangements, correspondence with social work or other relevant organisations.	

We will generally retain personal data of pupils for the duration of the relationship with us and for seven years afterwards.