



Northbourne Park School (including EYFS)

Data Protection Policy

Date created: September 2011

Last Reviewed: July 2026

Date for review: July 2028

Owned by: Headteacher

Reviewers: SMT

Approved by: F and GP Committee

Introduction

The UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA), the Privacy and Electronic Communications Regulations (PECR) and the The Data Use and Access Act 2025 (DUAA) is the law that protects personal privacy and upholds individual's rights. It applies to anyone who handles or has access to people's personal data.

This policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the legislation. It will apply to personal information regardless of the way it is used, recorded and stored and whether it is held in paper files or electronically.

Northbourne Park School keeps certain information about its employees, pupils and their parents to allow it to monitor performance, achievements and health and safety. In so doing, the School will comply with the terms of GDPR and the Data Protection Act and any subordinate legislation, to ensure personal data is treated in a manner that is fair and lawful. In summary, these state that personal data shall:

- Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met;
- Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
- Be adequate, relevant and not excessive for that purpose;
- Be processed in accordance with the data subject's rights;
- Be kept safe for unauthorised access, accidental loss or destruction;

The School and all staff or others who process or use personal information on the school's behalf must ensure that they follow these principles at all times. In order to ensure that this happens, the school has developed this data protection policy.

Status of this Policy

This policy does not form part of the formal contract of employment for staff or a formal offer of a place of study for pupils. However, it is a condition of employment or admission that employees and pupils' parents will abide by the rules and policies made by the School from time to time. Any failure to follow the policy can, therefore, result in disciplinary proceedings.

The Data Controller and the Data Protection Officer

The School as a body corporate is the Data Controller under GDPR and the 1998 Act and Data Control is managed by the Head teacher. The IT Manager will deal with the day-to-day matters. Any member of staff, pupil or any other individual who considers that the policy has not been followed in respect of personal data about himself or herself should raise the matter with the Head teacher in the first instance.

Data Gathering

All personal data relating to staff, pupils or other people with whom we have contact, whether held on computer or in paper files, are covered by the Act; only relevant personal data may be collected and the person from whom it is collected should be informed of the intended use of the data and of any possible disclosures of that information which may be made.

Data Checking

The School will issue regular reminders to staff and parents to ensure that personal data held is up-to-date and accurate.

Responsibilities of Staff

All staff are responsible for:

- Checking of any information which they provide to the School in connection with their employment is accurate and up-to-date;
- Informing the School of any changes to information they have provided, e.g. change of address, either at the time of appointment or subsequently. The School cannot be held responsible for any errors unless the staff member has informed the school of such changes.

Responsibility of Parents

The School Administrator and/or Admission Officer will remind pupils and their parents that all personal information provided to the school is accurate and up-to-date. Parents should ensure that changes of address, etc, are notified to the School. The School cannot be held responsible for any errors unless the parent has informed the School of such changes.

Subject to the above, any errors discovered will be rectified and, if the incorrect information has been disclosed to a third party, any recipients informed of the corrected data.

Data Storage

The Staff is responsible for ensuring that:

- Any personal information held in respect of pupils is kept securely;
- The personal information is not disclosed either orally or in writing or electronically or by any other means accidentally or otherwise to any unauthorised third party;
- Staff should note that any unauthorised disclosure will usually be a disciplinary matter.

Personal data should:

In respect of manual data, be stored in a secure and safe manner. It should be kept in a locked filing cabinet, drawer or safe where it is inaccessible to anyone who does not have a legitimate reason to view or process that data.

Electronic data should be stored coded, encrypted or password protected, whether held on a local hard drive or on a network drive that is regularly backed up; if a copy is kept on a diskette (or on other removal storage media) that medium must itself be kept in a locked filing cabinet, drawer or safe.

Wherever possible, computer workstations in administrative areas must be positioned so that they are not visible to casual observers waiting in the office. Always log off (or lock) Study machines when they leave them.

Data Processing

Before any processing activity starts for the first time, and then regularly afterwards, the purpose(s) for the processing activity and the most appropriate lawful basis (or bases) for that processing must be selected:

- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the school
- Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract
- Processing is necessary for compliance with a legal obligation to which the data controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- Processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party
- The data subject has given consent to the processing of his or her data for one or more specific purposes. Agreement must be indicated 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, the consent must be kept separate from those other matters

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured. Consent may need to be reviewed if personal data is intended to be processed for a different and incompatible purpose which was not disclosed when the data subject first gave consent.

The decision as to which lawful basis applies must be documented, to demonstrate compliance with the data protection principles and include information about both the purposes of the processing and the lawful basis for it in the school's relevant privacy notice(s).

When determining whether legitimate interests are the most appropriate basis for lawful processing (only where appropriate outside the school's public tasks) a legitimate interests assessment must be carried out and recorded. Where a significant privacy impact is identified, a data protection impact assessment (DPIA) may also need to be conducted.

Sensitive Personal Information

Processing of sensitive personal information (known as 'special categories of personal data') is prohibited unless a lawful special condition for processing is identified.

Sensitive personal information is data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or orientation or is genetic or biometric data which uniquely identifies a natural person.

- Sensitive personal information will only be processed if:
 - There is a lawful basis for doing so as identified on previous page
 - One of the special conditions for processing sensitive personal information applies:
 - the individual ('data subject') has given explicit consent (which has been clearly explained in a Privacy Notice)
 - the processing is necessary for the purposes of exercising the employment law rights or obligations of the school or the data subject
 - the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent
 - the processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim
 - the processing relates to personal data which are manifestly made public by the data subject
 - the processing is necessary for the establishment, exercise or defence of legal claims
 - the processing is necessary for reasons of substantial public interest
 - the processing is necessary for purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, the provision of social care and the management of social care systems or services
 - the processing is necessary for reasons of public interest in the area of public health.

Sensitive personal information will not be processed until an assessment has been made of the proposed processing as to whether it complies with the criteria above and the individual has been informed (by way of a privacy notice or consent) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it

Data Disposal

Unless there is a prior agreement that a member of staff at the School will act as a referee for a departing employee, all personal data relating to a member of staff will in normal circumstances be destroyed five years after that member of staff leaves the School.

All personal data relating to a pupil held in normal circumstances be destroyed five years after the pupil leaves the School

In certain exceptional circumstances, which will be a matter of formal record, the Headmaster can, in consultation with the SMT order that a personal file is retained beyond the point of normal destruction.

Other than at the discretion of the Headmaster and Governors, five years after a member of staff leaves the School their file will be closed and all retained records destroyed.

If some matter involving a member of staff or a pupil is *sub judice* at the time when closed data would usually be destroyed in accordance with this policy, the person holding the data on behalf of the School will pass the material on file to the Headmaster and Bursar, who will seek advice before proceeding with the disposal of that data.

The School will issue regular reminders to staff to ensure that data is disposed of at the proper time and in an appropriate manner

Team photographs, and other material celebrating an individual's achievement of distinction whilst a student (or member of staff) at the School will not be destroyed under these policy provisions but will be archived in the Strong Room. Some material may be displayed in a boarding house or other public display area within the school, before being passed (in time) to the Strong Room.

Medical records held by the local Practice will be disposed of in accordance with their policies and protocols.

Data for disposal will should be shredding or wiping prior to controlled destruction. Personal data relating to a member of staff or a pupil will never be disposed of in an unauthorised manner (e.g. using the weekly refuse collections).

Subject Access Request

All people for whom the School holds personal information are entitled to:

- Know what information the school holds and processes about them and why.
- Know how to gain access to it.
- Understand the mechanisms used to keep the data up-to-date.
- Know what the school is doing to comply with its obligations under the 1998 Act.

All people for whom the School holds personal information have a right under the 1998 Act to access certain personal data being kept about them either on computer or in certain files. If the School sees a *written* request from a data subject to see any or all personal data that the School holds about them, this will be treated as a subject access request and the School will respond within 40 days, as required by the 1998 Act.

GDPR and the Data Protection Act gives all school pupils, regardless of age, the right of access to their school pupil records. Requests to see or receive copies of records should be made in writing to the Headmaster.

In addition to the right to be given a copy of their *educational* record, pupils are entitled to be given a description of the *personal* data which is also part of the school record, together with: details of the *purposes* for which those data are processed; the *sources* of the data (if known); the individuals or organisations to which the data may have been *disclosed*.

A period of up to 15 school days is allowed in which to respond to a subject access request for educational records. (The equivalent period for other types of record is up to 40 days).

Pupils may be asked for information to verify their identity if it is necessary, for instance in the case of former pupils who may not be currently known to the School. They may also be asked for information necessary to locate the data held about them. For instance, a pupil may be asked to supply the dates between which he or she attended the School.

Only in exceptional cases will the School be able to withhold some of the information which is requested by a pupil. For example, information does not have to be disclosed by the School where that information might cause harm to the physical or mental health of the pupil or a third party. Also, information which may identify third parties (for example other pupils, although not teachers) is exempt from disclosure by the school. Information may also be withheld if in that particular case it would hinder the prevention and detection of crime or the prosecution or apprehension of offenders to provide it.

If pupils are incapable of understanding or exercising their own rights under GDPR and the Data Protection Act parents can make subject access requests on their behalf.

If a pupil or parent feels that the school is ignoring the subject access request, is refusing to disclose the information or has not given full disclosure of the information, the matter may be referred to the Information Commissioner.

Parents have an independent right of access to school pupil records (under the Education Pupil Information (England) Regulations 2000). Because of this, the pupils themselves have no right to prevent their parents from obtaining a copy of their school record.

Data Disclosures to Third Parties

Personal data will only be disclosed to organisation or individuals for whom consent has been given to receive the data, or to organisations that have a legal right to receive the data, or to organisations that have a legal right to receive the data without consent being given.

When requests to disclose personal data are received by telephone, it is the responsibility of the school to ensure that the school is entitled to disclose the data and that the organisation is who it says it is.

A record will be kept of any personal data disclosed so that the recipient can be informed if the data is later found to be inaccurate.

Personal data will not be used in newsletters, websites or other media without the consent of the data subject.

Information Security

The school will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. All staff are responsible for keeping information secure in accordance with the legislation and must follow their school's acceptable usage policy. Please refer to Northbourne Park School Information Security and Acceptable Use Agreement for Staff and Governors.

Data breaches

A data breach may take many different forms:

- Loss or theft of data or equipment on which personal information is stored
- Unauthorised access to or use of personal information either by a member of staff or third party
- Loss of data resulting from an equipment or systems (including hardware or software) failure
- Human error, such as accidental deletion or alteration of data
- Unforeseen circumstances, such as a fire or flood
- Deliberate attacks on IT systems, such as hacking, viruses or phishing scams
- Blagging offences where information is obtained by deceiving the organisation which holds it

The school must report a data breach to the Information Commissioner's Office (ICO) without undue delay and where possible within 72 hours, if the breach is likely to result in a risk to the rights and freedoms of individuals. The school must also notify the affected individuals if the breach is likely to result in a high risk to their rights and freedoms.

Staff should ensure they inform the DPO and Headmaster immediately that a data breach is discovered and make all reasonable efforts to recover the information, following the school's agreed breach reporting process.

Training

The school will ensure that staff are adequately trained regarding their data protection responsibilities.

Consequences of a failure to comply

The school takes compliance with this policy very seriously. Failure to comply puts data subjects whose personal information is being processed at risk and carries the risk of significant civil and criminal sanctions for the individual and the school and may in some circumstances amount to a criminal offence by the individual.

Any failure to comply with any part of this policy may lead to disciplinary action under the school's procedures and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

If you have any questions or concerns about this policy, you should contact your line manager or the school's DPO.

Data Protection Complaints

If you feel that your data protection rights have been infringed, you may submit a complaint to the school. Details of how to do this are set out in the school's Complaints Policy, available on the school website.

Review of Policy

This policy will be updated as necessary to reflect best practice or amendments made to the GDPR or DPA.

The Supervisory Authority in the UK

Please follow this link to the ICO's website (<https://ico.org.uk/>) which provides detailed guidance on a range of topics including individuals' rights, data breaches, dealing with subject access requests, how to handle requests from third parties for personal data etc.