Norfolk House School

DATA PROTECTION POLICY

This policy applies to all age groups in the school, including the EYFS

(in line with The EU General Data Protection Regulation (GDPR))

Norfolk House School

Date of Policy : April 2018

Reviewed: August 2025

Our Commitment:
Norfolk House is committed to the protection of all personal and sensitive data for which it holds responsibility as the Data Controller and the handling of such data in line with the data protection principles and the Data Protection Act (DPA).
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protectionprinciples/

Changes to data protection legislation (GDPR May 2018) shall be monitored and implemented in order to remain compliant with all requirements. The legal basis for processing data is that it is necessary to carry out these tasks in the public interest.

It is important that governing bodies and proprietors are aware that among other obligations, UK General Data Protection Regulation, the Data Protection Act 2018 and the Data (Use and Access) Act 2025 place duties on organisations and individuals to process personal information fairly and lawfully and to keep the information they hold safe and secure.

The member of staff responsible for data protection is Tej Lander.

The school is also committed to ensuring that staff are aware of data protection policies, legal requirements and adequate training is provided to them.

The requirements of this policy are mandatory for all staff employed by the school and any third party contracted to provide services within the school.

Notification:
Our data processing activities will be registered with the Information Commissioner's Office (ICO) as required of a recognised Data Controller. Details are available from the ICO:
https://ico.org.uk/about-the-ico/what-we-do/register-of-data-controllers/

Changes to the type of data processing activities being undertaken shall be notified to the ICO and details amended in the register. Breaches of personal or sensitive data shall be notified within 72 hours to the individual(s) concerned and the ICO.

Data Protection Individual Rights
Under GDPR the individual has the following rights, this policy and the associated GDPR Policies and Privacy notices held by the school are implemented to ensure these rights are upheld

- Right to be informed - Individuals have the right to be informed about the collection and use of their personal data.
- Right of access - Individuals have the right to access and receive a copy of their personal data, and other supplementary information.
- Right to rectification The UK GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.
- Right to erasure - The UK GDPR introduces a right for individuals to have personal data erased.
- Right to restrict processing - Individuals have the right to request the restriction or suppression of their personal data.
- Right to data portability - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- Right to object - The UK GDPR gives individuals the right to object to the processing of their personal data in certain circumstances.

Personal and Sensitive Data:
All data within the school's control shall be identified as personal, sensitive or both to ensure that it is handled in compliance with legal requirements and access to it does not breach the rights of the individuals to whom it relates.

The definitions of personal and sensitive data shall be as those published by the ICO for guidance:
https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions/

The principles of the Data Protection Act shall be applied to all data processed:
- ensure that data is fairly and lawfully processed
- process data only for limited purposes
- ensure that all data processed is adequate, relevant and not excessive
- ensure that data processed is accurate
- not keep data longer than is necessary
- process the data in accordance with the data subject's rights
- ensure that data is secure
- ensure that data is not transferred to other countries without adequate protection.

Fair Processing / Privacy Notice:
We shall be transparent about the intended processing of data and communicate these intentions via notification to staff, parents and pupils prior to the processing of individual's data. Notifications shall be in accordance with ICO guidance and, where relevant, be written in a form understandable by those defined as 'Children' under the legislation.

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/accountability-framework/transparency/

There may be circumstances where the school is required either by law or in the best interests of our students or staff to pass information onto external authorities, for example our local authority, Ofsted, or the department of health.

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of our school shall be clearly defined within notifications and details of the basis for sharing given. Data will be shared with external parties in circumstances where it is a legal requirement to provide such information.

Any proposed change to the processing of an individual's data shall first be notified to them. Under no circumstances will the school disclose information or data:
- that would cause serious harm to the child or anyone else's physical or mental health or condition
- indicating that the child is or has been subject to child abuse or may be at risk of it, where the disclosure would not be in the best interests of the child
- recorded by the pupil in an examination
- that would allow another person to be identified or identifies another person as the source, unless the person is an employee of the school or local authority or has given consent, or it is reasonable in the circumstances to disclose the information without consent. The exemption from disclosure does not apply if the information can be edited so that the person's name or identifying details are removed
- in the form of a reference given to another school or any other place of education and training, the child's potential employer, or any national body concerned with student admissions.

Data Security:
In order to assure the protection of all data being processed and inform decisions on processing activities, we shall undertake an assessment of the associated risks of proposed processing and equally the impact on an individual's privacy in holding data related to them. Risk and impact assessments shall be conducted in accordance with guidance given by the ICO:

https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/guide-to-accountability-and-governance/accountability-and-governance/data-protection-impact-assessments/

Security of data shall be achieved through the implementation of proportionate physical and technical measures. Nominated staff shall be responsible for the effectiveness of the controls implemented and reporting of their performance.

The security arrangements of any organisation with which data is shared shall also be considered and these organisations shall provide evidence of the competence in the security of shared data.

Sharing Data
Data may be disclosed to the following third parties without consent:

- Other schools If a pupil transfers from Norfolk House School to another school, their academic records and other data that relates to their health and welfare will be forwarded onto the new school as soon as possible and within 5 days. This will support a smooth transition from one school to the next and ensure that the child is provided for as is necessary. It will aid continuation which should ensure that there is minimal impact on the child's academic progress as a result of the move.
- Examination authorities This may be for registration purposes, to allow the pupils at our school to sit examinations set by external exam bodies.
- Health authorities; As obliged under health legislation, the school may pass on information regarding the health of children in the school to monitor and avoid the spread of contagious diseases in the interest of public health.
- Police and courts If a situation arises where a criminal investigation is being carried out we may have to forward information on to the police to aid their investigation. We will pass information onto courts as and when it is ordered.
- Social workers and support agencies In order to protect or maintain the welfare of our pupils, and in cases of child abuse, it may be necessary to pass personal data on to social workers or support agencies.
- Educational division schools may be required to pass data on in order to help the government to monitor the national educational system and enforce laws relating to education.

Data Rights Access to Information
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 be given access to your child's educational record, contact Tej Lander.

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, you should raise your concern with us in the first instance or directly to the Information Commissioner's Office at https://ico.org.uk/concerns/

Requesting access to your personal data - Subject Access Request Procedure
This document outlines the school's procedure for responding to Subject Access Requests (SARs), as required by data protection legislation.

Duty of the School Under a Subject Access Request
Upon receiving a valid Subject Access Request, the school has a duty to:

- Confirm whether it is processing personal data related to the individual
- Provide a copy of the personal data it holds.

Provide supplementary information, including:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients or categories of recipient to whom the personal data have been or will be disclosed
- The envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- The existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- The right to lodge a complaint with a supervisory authority.
- Where the personal data are not collected from the data subject, any available information as to their source.

Time Frames
The school will respond to a SAR
without undue delay, and in any event before the end of the applicable time period of one month beginning with the relevant time. The relevant time means the latest of the following

- when the controller receives the request in question;
- when the controller receives the information (if any) requested in connection with a request

Extension of Time Frame
The controller may, by giving notice to the data subject, extend the applicable time period by two further months where that is necessary by reason of

- the complexity of requests made by the data subject, or
- the number of such requests.

Within the context of a school the date of receipt of the request may create complications, if received in the scheduled holiday periods as key staff may not be available to process requests. Where the data controller advises the data subject of such a request be given before the end of the period of one month beginning with the relevant time, and state the reasons for the delay.

Pause in Time Frame
Where the controller reasonably requires further information in order to identify the information or processing activities to which a request relates

- the controller may ask the data subject to provide the further information, and
- the period beginning with the day on which the controller makes the request and ending with the day on which the controller receives the information does not count towards the applicable time period

Examples where a controller may reasonably require further information

- where the controller processes a large amount of information concerning the data subject.

- the request is historic

This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The data subject will be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

Redaction or Exemption of Data

There are certain categories of data that may not be shared, in line with the advice in this policy, the Information Security Policy and GDPR Privacy Notices.

The school may redact or exempt certain data from a SAR response under specific circumstances, primarily to protect the rights and freedoms of others, or where certain legal exemptions apply. These may include:

- Information identifying other individuals: Personal data of third parties will be redacted unless explicit consent is obtained from those individuals, or it is reasonable to provide the information without their consent.
- Legal professional privilege: Information subject to legal professional privilege is exempt from disclosure.
- Management information: Certain information held for management purposes, such as future plans or negotiations, may be exempt where disclosure would prejudice the conduct of the business.
- Criminal investigations: Information relating to ongoing or prospective criminal investigations may be exempt.
- Public interest: In some cases, information may be exempt if its disclosure would be detrimental to the public interest.

Any redactions or exemptions will be referred to in the above terms when responding to the SAR

Circumstances Under Which the School May Not Respond to a Subject Access Request

The school may refuse to act on a SAR in the following circumstances:

- Manifestly unfounded or excessive requests: If a request is clearly without any reasonable basis, or is repetitive in nature. The school may charge a reasonable fee or refuse the request entirely, providing a clear justification.
- Identity verification: If the school has reasonable doubts concerning the identity of the individual making the request, it may request further information to confirm their identity. The one-month period for response will not begin until the identity has been verified.
- Requests for information already provided: If the school has previously provided the same information to the same individual within a reasonable timeframe, and there has been no significant change to the data, the school may refuse to provide it again.

In all cases where the school refuses to act on a request, it will inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Information Commissioner's Office (ICO) and seeking a judicial remedy.

Photographs and Video:

Images of staff and pupils may be captured at appropriate times and as part of educational activities for use in school only. Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources. It is the school's policy that external parties (including parents) may not capture images of staff or pupils during such activities without prior consent.

Location of information and data:

Hard copy data, records, and personal information are stored out of sight and in a locked cupboard. The only exception to this is medical information that may require immediate access during the school day. This will be

stored with the school medical coordinator. Sensitive or personal information and data should not be removed from the school site, however the school acknowledges that some staff may need to transport data between the school and their home in order to access it for work in the evenings and at weekends. This may also apply in cases where staff have offsite meetings, or are on school visits with pupils.

The following guidelines are in place for staff in order to reduce the risk of personal data being compromised:

- Paper copies of data or personal information should not be taken off the school site. If these are misplaced they are easily accessed. If there is no way to avoid taking a paper copy of data off the school site, the information should not be on view in public places, or left unattended under any circumstances.
- Unwanted paper copies of data, sensitive information or pupil files should be shredded. This also applies to handwritten notes if the notes reference any other staff member or pupil by name.
- Care must be taken to ensure that printouts of any personal or sensitive information are not left in printer trays or photocopiers.
- If information is being viewed on a PC, staff must ensure that the window and documents are properly shut down before leaving the computer unattended. Sensitive information should not be viewed on public computers.

Data Disposal:

The school recognises that the secure disposal of redundant data is an integral element to compliance with legal requirements and an area of increased risk. All data held in any form of media (paper, tape, electronic) shall only be passed to a disposal partner with demonstrable competence in providing secure disposal services. All data shall be destroyed or eradicated to agreed levels meeting recognised national standards, with confirmation at completion of the disposal process.

Disposal of IT assets holding data shall be in compliance with ICO guidance:

https://ico.org.uk/for-organisations/advice-and-services/certification-schemes/certification-scheme-register/adisa-ict-asset-recovery-certification-80/

The school has identified a qualified source for disposal of IT assets and collections.