Oxford Sixth Form College

A NORD ANGLIA EDUCATION SCHOOL

Data Protection Policy

Revised August 2024

Review Date July 2025

1. Data protection principles

The College will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;
- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

2. Definitions

The following definitions shall apply to this policy:

"criminal records information" means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;

"data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;

"data subject" means the individual to whom the personal information relates;

"personal information" (sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;

"sensitive personal information" (sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

"processing information" means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;

"pseudonymised" means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual.

3. Basis for processing personal information

This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

- review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, i.e.:
    - that the data subject has consented to the processing;
    - that the 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;
    - that the processing is necessary for compliance with a legal obligation to which the College is subject;
    - that the processing is necessary for the protection of the vital interests of the data subject or another natural person;
    - that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or
    - that the processing is necessary for the purposes of legitimate interests of the College or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject.
- except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose);
- document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;
- include information about both the purposes of the processing and the lawful basis for it in our relevant Privacy Notice(s);
- where sensitive personal information is processed, also identify a lawful special condition for processing that information (see '**Sensitive Personal Information**' section below), and document it; and
- where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

When determining whether the College's legitimate interests are the most appropriate basis for lawful processing, we will:

- conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;
- if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);
- keep the LIA under review, and repeat it if circumstances change; and
- include information about our legitimate interests in our relevant Privacy Notice(s).

4. Sensitive personal information

The College may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

- we have a lawful basis for doing so as set out above, e.g. it is necessary for the performance of the employment contract, to comply with the College's legal obligations or for the purposes of the College's legitimate interests; and
- one of the special conditions for processing sensitive personal information applies, e.g.:
    - the data subject has given explicit consent;
    - the processing is necessary for the purposes of exercising the employment law rights or obligations of the College 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;
    - processing relates to personal data which is manifestly made public by the data subject;
    - the processing is necessary for the establishment, exercise or defence of legal claims; or
    - the processing is necessary for reasons of substantial public interest.

Before processing any sensitive personal information, staff must notify the Data Protection Administrator of the proposed processing, in order that they may assess whether the processing complies with the criteria noted above.

Sensitive personal information will not be processed until:

- the assessment referred to above has taken place; and
- the individual has been properly informed (by way of a Privacy Notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

The College's Privacy Notices set out the types of sensitive personal information that the College processes, what it is used for and the lawful basis for the processing.

5. Data Protection Impact Assessments (DPIA)

Where processing is likely to result in a high risk to an individual's data protection rights (e.g. where the College is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Before any new form of technology is introduced, the manager responsible should contact the Data Protection Administrator in order that they can consider whether a DPIA should be carried out.

6. Documentation and records

We will keep written records of processing activities which are high risk, i.e. which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information, including:

- the purposes of the processing;
- a description of the categories of individuals and categories of personal data;
- categories of recipients of personal data;
- where possible, retention schedules; and
- where possible, a description of technical and organisational security measures.

If we process sensitive personal information or criminal records information, we will keep written records of:

- the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;
- the lawful basis for our processing; and
- whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

We will conduct regular reviews of the personal information we process and update our documentation accordingly.

7. Privacy Notices

The College obtains, keeps and uses personal information about students, their families, alumni, staff, governors and suppliers of the College. The detail relating to how we collect and process that information is set out within separate Privacy Notices that can be found in the staff handbook and on the College website: https://www.oxfordsixthformcollege.com/the-college/policies/

We will take appropriate measures to provide information in Privacy Notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

It is important that all parties read and comply with the College's Privacy Notices.

8. Individual rights and obligations

All College stakeholders have a number of rights in relation to their personal information and these are set out within the Privacy Notices.

Individuals are responsible for helping the College keep their personal information up to date.

9. Information security

The College will use appropriate technical and organisational measures in accordance with the College's policies to keep personal information secure and, in particular, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. With the rise of AI please refer to NAE's AI Policy for guidance on best practice.

These may include:

- making sure that, where possible, personal information is pseudonymised or encrypted;
- ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Where the College uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

- the organisation may act only on the written instructions of the College;
- those processing the data are subject to a duty of confidence;
- appropriate measures are taken to ensure the security of processing;
- sub-contractors are only engaged with the prior consent of the College and under a written contract;
- the organisation will assist the College in providing subject access and allowing individuals to exercise their rights under the GDPR;
- the organisation will assist the College in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;
- the organisation will delete or return all personal information to the College as requested at the end of the contract; and

- the organisation will submit to audits and inspections, provide the College with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the College immediately if it is asked to do something infringing data protection law.

Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek approval of its terms by the Data Protection Administrator.

10. Storage and retention of personal information

Personal information (and sensitive personal information) will be kept securely in accordance with the College's Data Retention Policy.

Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained. Staff should follow the College's Data Retention Policy, which sets out the relevant retention period, or the criteria that should be used to determine the retention period. Where there is any uncertainty, staff should consult the Data Protection Administrator.

Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely. We may retain personal data for archiving purposes where it is necessary to do so in the public interest, for scientific or historical research purposes or statistical purposes subject to appropriate safeguards being put in place to protect the rights and freedoms of the data subject.

11. Data breaches

A data breach may take many different forms, for example:

- loss or theft of data and/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 failure (including hardware and software);
- human error, such as accidental deletion or alteration of data or sending data to the incorrect recipient;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

Data privacy compliance is everyone's responsibility and any suspected breach must be reported. Staff must follow the Data Breach Policy and Procedure available from the College website. https://www.oxfordsixthformcollege.com/the-college/policies/

- For a minor data breach that affects a low number of people, does not contain sensitive data and can be easily corrected or minimised, contact Marc.Lewis@oxfordsixthformcollege.com for advice.
- A more serious breach must be reported to the Principal and/or Director of Estates and Facilities as soon as possible. Failure to comply with this obligation could result in disciplinary action being taken.

The College will assess the severity of the data breach using the matrix contained within the Data Breach Policy, and if necessary:

- notify Nord Anglia's Global Compliance Officer of the details of the breach;
- notify the Chair of Governors of the details of the breach;
- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

12. International transfers

In most cases the College will not transfer personal information outside the UK or European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway. If staff wish to transfer personal information outside the UK and EEA they must consult with the Data Protection Officer (at Nord Anglia Education) before doing so. The Data Protection Officer will permit the transfer to happen only on the basis that either (i) the country, territory or organisation is designated as having an adequate level of protection, or (ii) the organisation receiving the information has provided adequate safeguards by way of standard data protection clauses or by compliance with an approved code of conduct.

13. Training

The College will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

14. Recruitment and staff

14.1 Scope

The principles of this policy apply to the personal information of job applicants and current and former staff, including employees, workers, volunteers, apprentices and contractors (collectively referred to as "**staff**" for the purposes of this policy).

Staff should refer to the College's Privacy Notices and other policies that relate to the use of internet, email, communications, social media and data retention available from

the College website. All staff must comply with the Data Protection Policy.

We will review and update this Data Protection Policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time.

It is important that you read and understand this policy because it gives important information about:

- the data protection principles with which the College must comply;
- your data protection obligations;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, e.g. about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

14.2 Recruitment data

The College obtains, keeps and uses personal information (also referred to as data) about job applicants and about current and former employees, workers, contractors, volunteers and apprentices for a number specific lawful purposes, as set out in the College's Staff Privacy Notice.

The Data Protection Administrator is responsible for data protection compliance within the College. If you have any questions or comments about the content of this policy or if you need further information, you should contact The Data Protection Administrator.

14.3 Criminal Records Information

Criminal records information will be processed in accordance with the College's Safer Recruitment Policy, available from the College website.
https://www.oxfordsixthformcollege.com/the-college/policies/

14.4 Individual obligations

Individuals are responsible for helping the College keep their personal information up to date. Staff should let the HR department know if the information held by the College changes, for example if a staff member moves house or changes the bank or building society account into which they are paid.

Staff may have access to the personal information of other members of staff, students, parents, suppliers, contractors and governors of the College in the course of their

employment or engagement. If so, the College expects staff to help meet its data protection obligations to those individuals. For example, staff should be aware that others also enjoy the rights set out above.

If a member of staff has access to personal information, they must:

- only access the personal information that they have authority to access, and only for authorised purposes;
- only allow other staff to access personal information if they have appropriate authorisation;
- only allow individuals who are not College staff to access personal information if they have specific authority to do so from the Data Protection Administrator;
- keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the College's e-Safety Policy.
- not remove personal information, or devices containing personal information (or which can be used to access it), from the College's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices.

14.5 **Reporting a breach or a concern**

Staff should report concerns or suspicions that one of the following has taken place (or is taking place or likely to take place):

- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions set out under the heading '**Sensitive Personal Information**' (section 4 above) being met;
- any data breach as set out under the heading '**Data Breaches**' (section 11 above);
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from the College's premises without appropriate security measures being in place; or
- any other breach of this Policy or of any of the data protection principles set out under the heading '**Data Protection Principles**' (section 1 above).

Failure to comply with the above obligations could result in disciplinary action being taken.

14.6 **Consequences of failing to comply**

The College takes compliance with this policy very seriously. Failure to comply with the policy:

- puts at risk the individuals whose personal information is being processed;
- carries the risk of significant civil and criminal sanctions for the individual and the College; and
- may, in some circumstances, amount to a criminal offence by the individual.

Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our 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.

15. Data Protection Administrator

Any questions or concerns about anything in this policy should be directed to the Data Protection Administrator Marc.Lewis@oxfordsixthformcollege.com. The Data Protection Administrator is responsible for monitoring compliance across the College and maintaining the data breach log.

16. Further policies and procedures

Oxford Sixth Form College is owned by Nord Anglia Education. Nord Anglia's over-arching data policies are available to staff from the Nord Anglia intranet:

- IT Security Policy
- Data Breach Response Policy
- Internal Data Privacy Policy
- Records Retention and Data Deletion policy
- AI Policy