Oxford Sixth Form College

A NORD ANGLIA EDUCATION SCHOOL

Data Breach & Procedure Policy

Revised August 2023

Review Date July 2024

This policy should be read in conjunction with the NAE Data Breach Response Policy and Procedures.

Policy statement

Oxford Sixth Form College holds large amounts of personal and sensitive data.

Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. This breach procedure applies to all personal and sensitive data held by Oxford Sixth Form College. This procedure applies to all College staff including volunteers, contractors and governing bodies, who are collectively referred to as 'staff'.

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

Purpose

This breach procedure sets out the course of action to be followed by all staff at Oxford Sixth Form College if a data protection breach takes place.

Legal context

Data security is a cornerstone of the EU General Data Protection Regulation (GDPR). The sixth data protection principle – the integrity and confidentiality principle – requires us to take appropriate technical and organisational measures to process personal data in a manner that ensures appropriate security including protection against:

- Unauthorised or unlawful processing; and
- Accidental loss, destruction or damage.

Types of breach

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Data protection breaches could be caused by a number of factors. Some examples are:

- loss or theft of data and/or equipment on which data is stored;
- unauthorised access to or use of personal information either by a member of staff or a 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 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 that holds it.

STEP ONE: Immediate Containment/Recovery

On discovery of a data protection breach, the following steps should be followed:

1. 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.

   If you discover a larger or more serious data breach, **immediately inform the Principal**, Vice Principal or the Director of Estates and Facilities, who in turn will inform the Data Compliance Administrator. If the breach occurs or is discovered outside normal working hours, this person should take all practical steps possible to inform the Principal or nominated representative as soon as possible.

   The **Data Breach Report Form** (see **Appendix 1**) should be completed and submitted as soon as possible after alerting the Principal to the breach.

2. **Containment and recovery.** The Principal (or nominated representative) must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant staff such as the IT Manager. The Principal will also inform the police where illegal activity is known or is believed to have occurred, or where there is a risk that illegal activity might occur in the future.

3. **Assess and record.** The College will undertake a detailed investigation of the breach as soon as possible and enter the incident on the data breach register. If the breach is deemed serious enough according to the Matrix in the Data Breach Assessment Form, the Principal (or nominated representative) will inform NAE's Global Compliance Officer (Jon Townsley) and the College's Chair of Governors (Patrick Horne). As a registered Data Controller, it is the College's responsibility to take the appropriate action and conduct any investigation. All incidents will be recorded on the College's Data Breach Log. Further information on investigations can be found in the Investigation section (Step Two below).

4. **Notify the Information Commissioner's Office (ICO).** Notification is required where the breach is likely to result in a risk to the rights and freedoms of individuals. Further information on ICO notification can be found in the Notification section (Step Three below).

5. **The Principal (or nominated representative) must quickly take appropriate steps to recover any losses and limit the damage.** Steps might include:

   a) Attempting to recover lost equipment.

   b) Contacting the relevant staff, so that they are prepared for any potentially inappropriate enquiries ('phishing') for further information on the individual or individuals concerned.

   c) Consideration should be given to a global email to all College staff.

   d) If an inappropriate enquiry is received by staff, they should attempt to obtain the enquirer's name and contact details (if possible) and confirm that they will ring the individual making the enquiry back. Whatever the outcome of the call, it should be reported immediately to the Principal (or nominated representative).

   e) Contacting the College's Marketing Department so that they can be prepared to handle any press enquiries. The Marketing Department can be contacted by telephone on 01865 793333 or via email at Lucy.Storey@oxfordsixthformcollege.com

   f) The use of back-ups to restore lost/damaged/stolen data.

   g) If bank details have been lost/stolen, consider contacting banks directly for advice on preventing fraudulent use.

   h) If the data breach includes any entry codes or IT system passwords, then these must be changed immediately and the relevant agencies and members of staff informed.

STEP TWO: Investigation

In most cases, the next stage would be for the Principal (or nominated representative) to fully investigate the breach as a matter of urgency. The Principal (or nominated representative) should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps need to be taken to remedy the situation. The investigation should consider:

- the type of data;
- its sensitivity;
- what protections are in place (e.g. encryption);
- what has happened to the data;
- whether the data could be put to any illegal or inappropriate use;
- how many people are affected;
- what type of people have been affected (pupils, parents, staff members, suppliers etc) and whether there are wider consequences to the breach.

The **Data Breach Assessment Form** (see **Appendix 2**) should be completed during the investigation to ensure all aspects are considered. The investigation should be completed as a matter of urgency and, wherever possible, within 5 days of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

A clear record should be made in the **Data Breach Log** of the nature of the breach and the actions taken to mitigate it.

Very minor incidents and Near Misses should still be recorded.

STEP THREE: Notification

The Data Breach Assessment Form (see **Appendix 2**) includes a matrix to help assess who should be notified, according to the severity of the breach.

The ICO and/or police may have already been notified as part of the initial containment. However, the decision to notify the ICO will normally be made once an investigation has taken place. The Principal (or nominated representative) will contact the Global Compliance Officer and Data Protection Officer at Nord Anglia Education (NAE) for expert legal advice about whether anyone should be notified of the breach. Every incident will be considered on a case by case basis. The following points will help the College to decide when and how to notify:

Should the College notify the ICO and/or affected individuals?

- Are there any legal or contractual requirements to notify?
- Will notification help prevent the unauthorised or unlawful use of personal data?
- Could notification help the individual(s) affected – could they act on the information to mitigate risks?
- How are individuals affected? This can include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised.
- If the breach is likely to result in a risk to the data subject's rights and freedoms the Data Protection Officer at NAE will **notify the ICO** on behalf of the College and will then act on the College's behalf in relation to any such correspondence. The ICO should only be notified if personal data is involved. There is guidance available from the ICO website and helpline on when and how to notify the ICO.
- If a breach is likely to result in a high risk to the rights and freedoms of individuals, the College or Data Protection Officer must **inform individuals concerned** directly and without undue delay. In other words, this should take place as soon as possible. Please note the threshold for informing data subjects is higher than for informing the ICO. Information on what might constitute a high risk to the rights and freedoms of individuals is available on the ICO website. This decision should also be made in consultation with the Global Compliance Officer and Data Protection Officer.

- Consider the dangers of over-notifying. Not every incident warrants notification and over-notification may cause disproportionate enquiries and work.
- Whether the incident is notifiable or not, it should be recorded in the organisations' data breach log.

How to notify the ICO and affected individuals

- **If it is deemed necessary to notify the ICO,** the Data Protection Officer at NAE will notify them on behalf of the College without undue delay, and not later than 72 hours after becoming aware of the breach. If it takes longer than this, the Data Protection Officer must give reasons for the delay.
- The notification should include a description of how and when the breach occurred, what data was involved and how many individuals are affected. The College should include details of what it has already done to mitigate the risks posed by the breach. Further information on what to include in a notification can be found on the ICO's website along with a form to be completed.
- **When notifying individuals**, the College or Data Protection Officer must give specific and clear advice on what they can do to protect themselves and what you are willing to do to help them. You should also give them the opportunity to make a formal complaint if they wish (see the College's Complaints Procedure, available from the College Website). https://www.oxfordsixthformcollege.com/wp-content/uploads/2022/12/OxSFC-Complaints-Policy-2022-23.pdf

If the College does not notify the ICO

- If the College decides not to notify the ICO, it must still record that decision and the reasons for it.

STEP FOUR: Review and Evaluation

The Principal (or nominated representative) should fully review both the causes of the breach and the effectiveness of the response to it. It should be written and sent to the next available Senior Management Team meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the breach warrants a disciplinary investigation, the manager leading the investigation should liaise with Human Resources for advice and guidance.

This breach procedure may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Consideration should be given to reviewing this breach procedure whenever the Data Protection Policy is reviewed.

Advice and assistance

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 by emailing Marc.Lewis@oxfordsixthformcollege.com.

*

Oxford Sixth Form College
A NORD ANGLIA EDUCATION SCHOOL

APPENDIX 1

DATA BREACH REPORT FORM

If you discover a data security breach, please act quickly.

- Notify the Principal and Director of Estates and Facilities immediately;
- Then complete this form as fully as possible and email it to the Principal Mark.Love@oxfordsixthformcollege.com within 2 hours of reporting the breach.

1 Details of the breach	
Date and time the breach was discovered and by whom:	
Person reporting the incident (name, email):	
Description of the breach – date, time, location, how the incident occurred, etc:	
If there has been a delay in reporting the incident, please explain the reason:	
2 Containment	
Is the breach contained or ongoing?	
If contained, date and time of containment:	
What steps were/will be taken to contain the breach?	
3 Personal data compromised	
Individuals whose data has been compromised (e.g. students, staff, parents, job applicants, etc):	
Number of data subjects affected:	
Details of any personal data compromised, and whether any is sensitive personal data [1]	
Are the affected individuals aware that the incident has occurred?	
4 Recovery	
If data is lost or stolen, what steps are being taken to recover the data?	

[1] Sensitive personal data is specifically: race/ethnicity, political/religious beliefs, Trade Union membership, physical/mental health or condition, sexuality/sex life, genetic data, biometric data where processed to uniquely identify an individual. For the purposes of data breach management, other information such as bank account details should also be classed as sensitive due to the risk of fraud.

Oxford Sixth Form College
A NORD ANGLIA EDUCATION SCHOOL

APPENDIX 2

DATA BREACH ASSESSMENT FORM

To be completed during the assessment process following a data breach.

Date of assessment meeting:	**Staff present:**

1 Details of the breach	
Date and time of breach:	
Brief description of the breach and its discovery:	
Details of any 3rd party service providers involved in the breach:	
2 Containment	
How much time elapsed between breach and containment?	
What steps were taken to contain it?	
What is known about the perpetrator?	
3 Personal data compromised	
Individuals whose data has been compromised (e.g. students, staff, parents, job applicants etc):	
Details of any personal data compromised, and whether any is sensitive personal data [2]	
Are the affected individuals aware that the incident has occurred?	
Have any affected individuals complained about the incident?	

[2] Sensitive personal data is specifically: race/ethnicity, political/religious beliefs, Trade Union membership, physical/mental health or condition, sexuality/sex life, genetic data, biometric data where processed to uniquely identify an individual. For the purposes of data breach management, other information such as bank account details should also be classed as sensitive due to the risk of fraud.

4 Recovery	
If data is lost or stolen, what steps are being taken to recover the data? If already recovered, when was the data recovered?	
5 Reporting	
Does NAE's **Global Compliance Officer** need to be notified? *(yes if assessed serious enough by the College)*	
Does the **Chair of Governors** need to be notified? *(yes if amber or red in the matrix below and assessed serious enough by the College)*	
Does the **ICO** need to be notified? *(yes if amber or red in the matrix below and assessed serious enough by the College)*	
Do **compromised individuals** need to be notified? *Consider if the distress and worry would be greater than the damage to personal security.*	
Any further action to be taken?	

DATA BREACH MATRIX

Risk scoring is achieved by multiplying probability against impact.

		IMPACT				
		TRIVIAL	**MINOR**	**MODERATE**	**MAJOR**	**EXTREME**
PROBABILITY	**RARE**	LOW	LOW	LOW	MEDIUM	MEDIUM
	UNLIKELY	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
	MODERATE	LOW	MEDIUM	MEDIUM	MEDIUM	HIGH
	LIKELY	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH
	VERY LIKELY	MEDIUM	MEDIUM	HIGH	HIGH	HIGH

When assessing **impact** look at what the actual impact and damage to the individual concerned is.

When assessing **probability**, assess what is the likelihood of this breach happening again.

Impact criteria explained

IMPACT CRITERIA				
Trivial	Isolated local negative perception.	Affects small number of people (<10)	Negligible regulatory/commercial/ contractual breach. Breach not reportable.	1
Minor	Sustained local negative perception.	May involve > 11 data subjects – no sensitive data	Minor regulatory/commercial/ contractual breach.	2
Moderate	Sustained local and/or regional and/or national perception.	May involve 100+ data subjects or relates to sensitive data	Regulatory censure and/or commercial/contractual breach. Reportable.	3
Major	Sustained regional and/or national perception.	May involve 500+ data subjects or relates to sensitive data	Regulatory fines and/or significant corporate breach.	4
Extreme	Sustained negative national perception.	Affects significant number of data subjects (>1000+). Remediation is likely to be time consuming and complex and related to sensitive information.	Corporate litigation.	5

Probability criteria explained

PROBABILITY CRITERIA		
Rare	One-off incident will not be repeated	1
Unlikely	May happen again, but remedial actions make this unlikely	2
Moderate	Could happen again, but remedial action has reduced this likelihood	3
Likely	Is likely to happen again within 1 to 7 days unless action is taken	4
Very likely	Is likely to happen again almost immediately unless action is taken ASAP	5