OXFORD International College

A NORD ANGLIA EDUCATION SCHOOL

DATA BREACH POLICY

POLICY INTENDED FOR:	Staff, Students and Parents
CATEGORY:	Data Protection
POLICY IMPLEMENTED BY:	Principal
POLICY MONITORED BY:	Data Protection Officer (DPO)
REVIEWED BY:	DPO, Principal
CONSULTATION WITH:	Senior Leadership Team (SLT)
REVIEW DATE:	June 2025
FUTURE REVIEW:	June 2026

The Three Pillars

The three pillars of Oxford International College (OIC) are:

- Academic Excellence
- Personal Development
- Career and University Pathways

CONTENTS

INTRODUCTION

This policy outlines the way Oxford International College (OIC) deals with any breaches involving personal data for which OIC is data controller and/or data processor. This policy has been written to work alongside the Data Protection Policy[1], IT security policies and protocols (e.g. Nord Anglia Education's (NAE) Information Security Policy and Information Security Incident Management) and Nord Anglia Education's Group Crisis Communication Manual.

Personal Data Breaches (Data Breach) are incidents that lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, Personal Data transmitted, stored or otherwise processed by OIC or processed on its behalf by a third-party data processor. We acknowledge that a Data Breach may also be a Security Incident as defined in the Information Security Policy in which case this policy will supplement the Security Incident protocols set out therein.

This policy details our reporting and notification requirements in a Data Breach, we have to determine whether we must notify the relevant Data Protection Authority ("DPA") and the individuals concerned. Unless a Data Breach is "Unlikely to result in a risk to the rights and freedoms of the persons involved", we have 72 hours from when we first had reasonable degree of certainty that a Data Breach had occurred to notify the UK's Information Commissioner's Office of the Data Breach.

SCOPE

This policy applies to all individuals working for or on behalf of the OIC at all levels and grades, including senior managers, officers, directors, employees (whether permanent, fixed term or temporary), consultants, contractors, trainees, seconded staff, homeworkers, casual workers and agency staff, volunteers, interns, agents, sponsors, or any other person associated with us, or any of our subsidiaries or their employees, wherever located (collectively referred to as "workers" in this policy).

INTERNAL RESPONSE TEAM

All Data Breaches should be reported to the OIC Data Protection Officer and Principal immediately who will determine the severity of the Breach and what type of response is required. They will inform and convene the Internal Response Team of which they form part in addition to:

- NAE Group Data Protection Officer or Global Compliance Manager
- NAE Chief Information Officer and Regional IT Lead
- Regional Managing Director

PROTOCOL

The Regional and Central Communications Team must always be alerted - they will provide advice, support and approve all internal and external communications.

Any information flow must be controlled:

[1] The defined terms used in the Data Protection Policy apply here also.

- **Incoming** information both to the response team and OIC must be centralized - please name one person (typically the DPO or Group DPO) who will provide accurate and timely updates to the Regional Managing Director (who will liaise with the Internal Response Team) and Central Communications
- **Outgoing** information to key stakeholders, especially media, regulators and any affected individuals must come from one source. All communication is approved and controlled from NAE Head Office. All statements must be reviewed by Internal Response Team and signed off by NAE Heads of Communications and Legal and agreed by the Group CEO.

DATA BREACH LOG

Details of all Data Breaches (including the cause, what took place and, where applicable, the Personal Data affected) and OIC's response (and reasons for those responses) should be recorded in a dedicated register for Data Breaches. Please note that this register may have to be provided to the relevant DPA on request. Details of Data Breaches and should be recorded whether any notifications were made or not. In cases where notification is not considered necessary, OIC should record the reasons for this. It is the DPO's responsibility to maintain the register of Data Breach.

Steps to follow

1. Discovery of Data Breach

Internal discovery and escalation. Upon discovery of the Data Breach (or a suspected Data Breach), the Breach should be notified to:

- OIC's Data Protection Officer
- Principal
- School IT Manager (if also a Security Incident)

Group Data Protection Officer or Global Compliance Manager must also be informed immediately; they may, based on the severity of the incident, have to notify our insurance providers.
If the event is deemed to be of a serious nature, it must be immediately referred to the:

- NAE Chief Information Officer
- Chief Legal Officer; and
- Regional Managing Director.

The Regional Emergency Plan should be deployed if the event is of a serious nature.
Notification received from Processor acting on OIC's behalf. Processors (e.g. our service providers) are required to notify us without undue delay after becoming aware of a Data Breach (whether it is unlikely to result in a risk to an individual's rights and freedoms) and if we receive a notification from one of our providers the above steps should be followed.
It is important to involve the NAE Legal Team early on for the purposes of establishing lawyer-client privilege.

2. Establish Client Lawyer Privilege

Lawyer-client privilege should be established and formalised as soon as possible after OIC/NAE becomes aware of a Data Breach (whether using internal or external counsel).

- All communications should be headed "Legally privileged and confidential". This can be included in email subject lines.
- There should be a clear separation between the technical investigation/ reporting and any form of legal analysis or comment on law/regulation.
- Advice from outside vendors, such as forensic professionals, should be routed through internal counsel so that OIC may argue that its communications are protected under privilege.

3. Coordinate the core internal response team

Contact the internal response team to arrange an initial "incident briefing" call/Email.
If this is within this is to be led by the OIC Data Protection Officer or the NAE Data Protection Officer if the incident is more serious.

4. Contain the incident and make an initial assessment

Note not all Data Breaches are Security Incidents and vice versa

- Investigate Security. As soon as possible after discovery of a Security Incident, the IT team should investigate whether the Security Incident is ongoing, whether the method, such as

malicious code, used to perpetrate the Security Incident is still active and whether the vulnerability is still present and exploitable.

- If also a Security Incident, determine if Personal Data has been affected - As soon as possible following discovery of a Security Incident (i.e. within 24 hours), the IT team should establish with a reasonable degree of certainty whether the Security Incident has led to Personal Data (i.e. information relating to an identified or identifiable individual) being compromised. If it has, the Security Incident shall be a " Data Breach" and we must immediately consider the items listed in section 7 below.
- **All Data Breaches** Contain and eliminate the breach. The IT team should take action to secure any data impacted by the Security Incident, eliminate the source and any vulnerabilities. In a non-Security Incident the responsible manager in coordination with the DPO must take all reasonable steps such as, but not limited to, recalling errant emails, disabling lost laptops or other devices, etc.
- Record of Data Breach. Keep and maintain a record of the Data Breach. See section 10 for more information.
- Status report. DPO to brief the internal response team on the findings of the initial assessment to help the response team assess the severity of the breach and next steps.

5. Wider Incident Response Team - Formation and Activation

- **Multi-disciplinary efforts**. The Data Breach may impact many different stakeholders within OIC or across NAE. Therefore, the initial response team may need to be expanded to ensure the input and involvement of other internal stakeholders.
- **External advisors**. Consider whether to involve external advisors in the incident response team. The external advisors would typically include lawyers and forensic professionals. In addition, the team may include credit monitoring and ID protection vendors, call centre vendors and PR firms.

6. Ongoing Investigation

IT assessment (when Security Incident). The IT team (in consultation with the incident response team) should make a more detailed assessment of:

- how the Security Incident occurred, including cause and vulnerabilities at issue;
- the data or systems that were impacted;
- identity of third parties that may have been impacted or harmed because of the Security Incident (e.g. clients, customers, employees, etc.);
- parties that may have been responsible for the breach (e.g. third party service providers, internal employees, etc.);
- whether Personal Data, trade secrets, IP or other sensitive information were compromised;
- whether the data was encrypted;
- if Personal Data is involved, the number of individuals impacted and where they are located; and
- how to permanently eliminate the cause of the Security Incident or remediate the vulnerability or problem that allowed the security breach to occur.

Collect evidence during IT assessment. If applicable, collect and preserve forensic evidence that is available, including evidence that may be relevant to actual or potential litigation.

7. Personal Data Breaches - Notification and Record Keeping

- **General**. Personal Data Breaches are Security Incidents that lead to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by NAE, or a processor acting on its behalf.
- **Notification requirements** - If the security incident is a Data Breach, the OIC's Data Protection Officer in conjunction with the Internal Response Team must determine whether it must notify the relevant data protection authority and whether it must notify the individuals concerned.
- **Notification to DPA** - Unless a Data Breach is "unlikely to result in a risk to the rights and freedoms of natural persons", OIC/NAE has 72 hours from when it first had a reasonable degree of certainty that a Data Breach had occurred to notify the DPA of the breach.

We should consider the following in determining the level of risk:

- the type of breach
- the nature, sensitivity and volume of Personal Data
- the ease of identification of individuals
- the severity of consequences for individuals
- special characteristics of the individuals
- the number of affected individuals

Please note that the risk threshold that triggers notification to a DPA is quite low. Some illustrative scenarios and guidance on when to notify are set out in Appendix 1. Any question around whether the risk threshold has been met should be referred to the NAE Legal Team and/or external counsel.

When notifying a DPA, we must provide the following information

- the nature of the Data Breach, including categories and approximate number of data subjects and Personal Data records concerned
- contact point within OIC/NAE for more information
- likely consequences of the Data Breach in particular on the affected individuals
- measures taken, or proposed to be taken, to address the Data Breach

Please note that, if all this information is not available within the first 72 hours, OIC/NAE can provide the relevant information in phases when it becomes available, e.g. following in-depth forensic investigations. OIC/NAE must give the relevant DPA reasons for the delay in providing further information.

If OIC/NAE is delayed in making an initial notification to the relevant data protection authority by more than 72 hours then, as with providing information in phases, it will have to provide reasons for the delay.

- **Notification to the individuals concerned**. Where the Data Breach is "likely to result in a high risk to the rights and freedoms of natural persons", OIC must communicate the Data Breach to the individual without undue delay unless:
    - OIC has applied measures that mean that the Personal Data is unintelligible to any person, e.g. encryption;

- Immediately following a breach, OIC has taken steps to ensure that the high risk is no longer likely to materialise; or
- It would involve disproportionate effort to contact individuals (in which case, a public announcement should be made to that effect).

The threshold for notifying individuals of the breach is higher than for notifying DPAs, but the same items as are listed above should be considered in determining the risk. Please also refer to Appendix 1 for examples of when notification may be required.
The notification should include:

- A clear description of the nature of the Data Breach, its likely consequences and any mitigating action taken; and
- The name and contact details of the Data Protection Officer.

Any external communications must be reviewed by the Central Communications department.

8. Other notifications to consider

- **Notify controllers**. Where OIC acts as a "processor", it must ensure relevant parties are notified in accordance with the terms of its processor agreement.
- **Law enforcement**. Consider whether a notification to the police / serious organised crime agency is appropriate or required. While there is no obligation the UK to report incidents to law enforcement agencies, doing so can lead to law enforcement investigating the matter and, in a best-case scenario, bringing a successful prosecution against any wrongdoers. Informing law enforcement also allows the authorities to develop a clearer picture of the types of cyber-crime that are happening in particular sectors.

Others

- **Banks** - If unauthorised payments have been made consider contacting banks to inform of unauthorised payments.
- **Third Parties** - If OIC has entered into any contractual terms which require OIC to inform its counterparties or third parties of matters such as Data Breaches, make notification to those parties.
- **Individuals** - When notifications are made to affected individuals under section 7 above, consider whether to offer credit monitoring and ID protection services to those individuals so that they can protect themselves against identity theft and/ or fraud.
- **Others** - Where Parents/Guardians or third-party organisations such as local authorities, child protection agencies, extra-curricular providers or insurers are required to be informed, make notifications to the extent required within required timeframes.

9. Claim/Regulatory Defence Phase

In the event a claim, demand, lawsuit or regulatory action arises out of a Data Breach consider engaging outside counsel to advise on the defence of the relevant claim.

10. Records and log of data breaches

Details of all Data Breaches (including the cause, what took place and, where applicable, the Personal Data affected) and OIC's response (and reasons for those responses) should be recorded in a

dedicated register of data breaches. Please note that this register may have to be provided to the relevant DPA on request. Details of the data breach and should be recorded whether any notifications were made or not. In cases where notification is not considered necessary, OIC should record the reasons for this.
OIC must retain its own data breach register and ensure that NAE's Central Compliance Team has sufficient information to add the Data Breach to the Global incident register.

EXAMPLES OF A DATA BREACH

Personal data breaches can include, but not limited to, the following:

- access by an unauthorised third party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending personal data to an incorrect recipient.
- computing devices containing personal data being lost or stolen.
- alteration of personal data without permission.
- loss of availability of personal data.

FURTHER INFORMATION

For further information about Data Breach Policy at OIC please speak with OIC Data Protection Officer.

dpo@oxcoll.com
Data Protection Officer
Oxford International College
1 London Place
OX4 1BD

APPENDIX - EXAMPLES OF PERSONAL DATA BREACHES AND WHO TO NOTIFY PROVIDED BY THE ARTICLE 29 DATA PROTECTION WORKING PARTY

Example	Notify the supervisory authority?	Notify the data subject?	Notes/recommendations
i. A controller stored a backup of an archive of Personal Data encrypted on a USB key or CD. The USB key or CD is stolen during a break- in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist, and the unique key is not compromised, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated.	Yes, report to competent supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the Personal Data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable Personal Data breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only functionality was to encrypt the data, and that there was no other malware present in the system.	Yes, report to the competent supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, depending on the nature of the Personal Data affected and the possible effect of the lack of availability of the data, as well as other likely consequences.	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority orto individuals as there would have been no permanent loss of availability or confidentiality. However, the supervisory authority may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a Personal Data breach has occurred and if it is a systemic flaw so that other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross- border processing.	Yes, as could lead to high risk	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.

vii. A website hosting company (a data processor) identifies an error in the code which controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	As the processor, the website hosting company must notify its affected clients (the controllers) without undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore, is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority	If there is likely no high risk to the individuals, they do not need to be notified.	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS Directive). If there is no evidence of this vulnerability being exploited with this particular controller a notifiable breach may not have occurred but is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for a period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high- risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal Data of a large number students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of Personal Data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in "to:" or "cc:" field, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of Personal Data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.