OXFORD International College

A NORD ANGLIA EDUCATION SCHOOL

DATA RETENTION POLICY

POLICY INTENDED FOR:	Staff
CATEGORY:	Data Protection
POLICY IMPLEMENTED BY:	Principal/ Governors
POLICY MONITORED BY:	Operations Manager
REVIEWED BY:	Operations Manager, Principal
CONSULTATION WITH:	Senior Leadership Team (SLT)
REVIEW DATE:	June 2024
FUTURE REVIEW:	June 2025

The Three Pillars

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

- Academic Excellence
- Personal Development
- Career and University Pathways

CONTENTS

INTRODUCTION

School information, records and data are vital assets. However, we do not need to retain all data and records indefinitely, and retaining data can expose us to risk as well as be a cost to our business. They must be created, organised, secured, maintained, and disposed of in compliance with legal and regulatory requirements, in a way that protects their content, and in a way that allows us to extract their full value.

This Records Retention Policy applies to all electronic data and paper-based filing systems maintained by or on behalf of Oxford International College (OIC). The Policy is designed to ensure that we:

- Comply with applicable laws and regulations to retain data;
- Comply with data protection obligations, in particularly to keep personal data no longer than is necessary for the purposes for which hit is processed (storage limitation principle);
- Handle, store and dispose of data responsibly and securely;
- Create and retain data where we need this to operate our business effectively, but we do not create or retain data without good reason;
- Allocate appropriate resources, roles and responsibilities to data retention;
- Regularly remind staff of their data retention responsibilities;
- Regularly monitor and audit compliance with this policy and update as required.

To ensure compliance, OIC will maintain a Process for Deletion and Retention of Data which will contain a schedule which sets out the retention periods for all their records ("Retention Schedule") which adheres to the principles and rules set out in in this Policy (held in both electronic and paper-based form).

This policy outlines the key principles that govern records retention within OIC and details the mandated retention periods of different categories of information. All employees are required to read and comply with the contents of this policy where relevant to their function(s).

ROLES AND RESPONSIBILITIES

All staff must comply with this policy, the Retention Schedule, any communication suspending data disposal and any specific instructions from the OIC Principal / OIC Data Protection Officer / Central Data Protection Officer and/or the Central Legal Team. Failure to do so may subject us, our staff and contractors to civil and/or criminal liability. An employee's failure to comply with this policy may result in disciplinary action, including suspension or termination.

Responsibility for the operational of the policy within OIC rests with each Head of Department and they are responsible for reviewing compliance with the policy at the end of each academic year for the data.

GENERAL PRINCIPLES

We should treat all records in accordance with the following retention principles:

a) Keep all company records subject to local mandatory retention periods;
b) Retain all company records that may be relevant to any notified regulatory investigation contemplated or active legal proceedings;
c) Retain in a recoverable format all company records for which there is an identifiable and ongoing business need; and

d) Appropriately dispose of all records that do not fall under a) to c) above.

Records that fall under principles a) to c) above should be securely maintained and controlled to prevent unauthorised access and safeguarded to ensure OIC's continued operation in the event of any incident affecting business continuity.

Where records are sent to third party organisations to handle or store, we should ensure those organisations are required to comply with paragraph 5 below. In addition, our arrangements with them must be adequate to enable compliance with principles a) to d) in relation to the records they hold. Storage of records with third parties does not discharge our responsibility to ensure records are retained and disposed of according to the requirements of this policy.

Records potentially relevant to:

- ongoing or potential legal or regulatory action;
- ongoing subject access request;
- ongoing investigation (internal or external);
- ongoing or planned audit (internal or external); or
- any other legal demand or requirement,

must not be deleted / destroyed. This is regardless of the retention period in set in the Retention Schedule.

If the records include any electronic files, then IT must be notified so as to take action to prevent any potential scheduled deletion.

PERSONAL DATA

Data Privacy Policy applies to all personal data, even if archived. Key data privacy principles that are applicable to data retention are as follows:

- Do not keep personal data any longer than necessary.
- Personal data that should be kept must not be deleted.
- Ensure that any personal data that is archived under this Policy is easily accessible to enable timely responses to 'data subject' access requests.

Remember that any retained personal data can become inaccurate or out of date and therefore only keep the minimum data necessary to achieve the ongoing legitimate purpose may be retained.

Adequate security measures needs to be in place to protect any personal data that is archived and additional security measures must be put in place for any Special Categories of Personal Data or Criminal Convictions Data.

Data retention of back-ups containing personal data is permissible under data protection laws. However, reasonable controls should be in place to ensure such data is destroyed after retention periods relating to the personal data have expired, or, if that is not practical, because critical business data is combined with personal data, or otherwise, appropriate controls must be in place to block access to personal data

included in the archives or back-up once a reasonable retention period relating to that personal data has expired.

FURTHER INFORMATION

For further information about Data Retention at OIC please speak with the OIC Data Protection Officer.

contact@oxcoll.com

Oxford International College
1 London Place
OX4 1BD