Data Storage and Protection Policy

Introduction

This policy outlines the lawful way Oxford International College (OIC) store personal information and the correct procedures to follow to ensure your data is secure. This policy has been written in line with the General Data Protection Regulations (GDPR) which come into effect as of 25 May 2018.

What is personal Information?

Personal information is information that the College collects which is specific to an individual. This includes, but is not limited to, Name, date of Birth, address, language and nationality. We hold academic information, including information from previous institutions such as relevant examination results for all students. Other personal information held by the College includes, but is not limited to, relevant medical information, behavioural & attendance records and special educational considerations. Personal information also includes any photographs or video footage of individuals. The College holds personal information on previous, prospective and current students as well as previous, prospective and current staff members.

How OIC Store Personal Data

All data relevant to students is held first and foremost on our Management Information System (MIS). This system is GDPR compliant and utilises high levels of security to protect the stored data it holds. Any data held outside of the MIS system will be appropriately protected or encrypted as relevant.

Data may be held by, or shared with, third party suppliers. Such suppliers are all checked to be GDPR compliant and data is shared through secure means.

How OIC Protect Personal Data

Please see below list of data storage points utilised by the college and the relevant security measures taken by the college to protect these:

Hard Copy Files:	Locked drawers or cabinets, locked rooms and locked storage areas
USB Sticks:	Password protected, stored in locked drawers/cabinets
Laptops:	Password protected, kept with owner when offsite or within locked premises/vehicle
External Hard Drives:	Password Protected, stored in locked drawers/cabinets
Mobile Phones:	Password Protected

Secure Password Creation & Storage

Where possible, passwords used to protect personal data will be alpha numeric, using both capital & lower case and at least 1 special character. Where possible capitalising of a letter or letters within a word will be used to increase security, as well as the use of a number in place of a letter within a word. For example:

£c1aiRe*5tronG18

Where alphanumeric passwords are not possible, such as on a mobile telephone, we will ensure that numeric passwords are not easily identifiable. Therefore, we do not use sequential numbered passwords (such as 123456) or the owners own birth date.

Storage of passwords will be within password protected and/or encrypted data bases only or using a secure third-party program or app designed for such storage.

Personal passwords are not written down or routinely shared between staff with the exception of the College IT administration who have ability to access such information only if required.

Encryption

Where personal data of any description is shared via email encryption should be used. Please see full encryption information sheet to show what encryption should be used and for step-by-step instructions on how to set this up.

Wherever possible when sharing personal data within the College the MIS emailing system should be used. If you are sharing information through the MIS no additional encryption is required.

Further information

If you have any questions about Data Protection at Oxford International College, please contact:

claire.wellstood@oxcoll.com
Operations Manager
Oxford International College
1 London Place
Oxford
OX4 1 BD

If you have a data protection concern that cannot or have not been resolved by the College, you have the right to raise it with the Information Commissioner's Office.