Data Breach Policy and Procedure

Revised: July 2022

Review date: July 2023

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

DATA BREACH POLICY AND PROCEDURE

Policy Statement

OxSFC holds large amounts of personal and sensitive data. Whilst every care is taken to protect personal data, we recognise that not all data protection breaches can be avoided. Therefore, we are prepared to take quick and decisive action to contain, recover, learn lessons to minimise any harm to individuals and the business. This procedure applies to all College staff including volunteers, contractors and governing bodies which are referred to as 'staff'.

Purpose

This breach procedure sets out the course of action to be followed by all staff at OxSFC if a data protection breach takes place. This policy is supplemental to the Nord Anglia Education Data Breach Response Policy and Information Security Incident Management procedures.

Key Additional steps:

These steps are to be performed in addition to those set out in the NAE Data Breach Response Policy and Information Security Incident Management procedures

1. Inform the Principal or nominated representative.

   In addition to the individuals listed it the NAE policy and procedures. Notice of any data protection breach must be immediately notified to the Principal or, in their absence, the Vice Principal.

2. Inform the College's Marketing Department.

   Ensure that the College's Marketing Department is notified so that they can work with NAE's Head of Communications or delegate. Email: Lucy.Storey@oxfordsixthformcollege.com

3. Any notifications to families will be managed by the College.

   The decision to notify families or individuals affected will be made by the Principal and they will appoint a team to manage such notifications.

4. Review and Evaluation post breach response

   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 SMT meeting for discussion. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right

5. The college will maintain a record of all breaches

   The Data Protection Officer will maintain a record of all breaches for the College

6. The college has an obligation to preserve records which contain information about allegations of sexual abuse for the Independent Inquiry into Child Sexual Abuse (IICSA), for the term of the inquiry (further information can be found on the IICSA website). All other records should be retained at least until the accused has reached normal pension age or for a period of 10 years from the date of the allegation if that is longer.

Advice and assistance

The Data Protection Officer 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 Officer (Marc Lewis) by calling 01865 793333 or emailing Marc.Lewis@oxfordsixthformcollege.com .

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 which holds it.