



## DATA PROTECTION – BREACH INVESTIGATION GUIDELINES

### Policy Statement

The College is committed in all its actions to comply with the General Data Protection Regulation (2018) and its amendments, will put in and place responsibilities and processes that underpin this commitment.

### 1. Introduction

The UK GDPR regulations dictate the way in which the College must manage any incidents where personal or sensitive data may have been lost or distributed incorrectly. The UK GDPR definition of a breach is 'A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.'

### 2. Process

The College has a data Incident Reporting process in place, and this is found on the College Intranet (OnePlace), where there are details of what a staff member needs to do to ensure that the Data Protection Team are notified of any incidents as soon as they have been highlighted of the issue.

There is an Incident Report Form to complete and this is emailed to the College GDPR team using the email [gdpr@burnley.ac.uk](mailto:gdpr@burnley.ac.uk), which is checked regularly.

Once an incident is reported, then that data protection team, led by the Data Protection Officer (DPO), must undertake an immediate investigation of the facts which must include:

- The data that has been affected
- The type of data
- The nature of the data (personal, sensitive ....)
- Details of the incident
- Details of the data subject(s)
- Who reported the incident
- When the incident was reported

As part of the investigation, the DPO may need to conduct an interview with any staff members who were involved in the incident, and also the data subject(s). Once the investigation has been completed, the DPO must establish whether the data incident is actually a 'Data Breach', and if so, whether the Information Commissioners Office (ICO) needs to be notified.

### 3. Action

Details of the data incident/breach must be recorded in the central Data Incident system, and the decision relating to ICO notification must be recorded together with all appropriate rationale.

