CLARE HALL
CAMBRIDGE

Data Breach Notification Policy

Aim

Clare Hall ('the College') is aware of the obligations placed on us by the General Data Protection Regulation (GDPR) in relation to processing data lawfully and to ensure it is kept securely.

One such obligation is to report a breach of personal data in certain circumstances and this policy sets out our position on reporting data breaches.

Data Breach

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of (or access to) personal data.
This will also apply to whichever process the personal data is breached – whether being transmitted, stored or processed.
Examples of data breaches:

- inadvertently disclosing personal data to an external party;
- theft or accidental destruction;
- accidental publication of personal data;
- sending an email containing personal data to the wrong person;
- accidentally disclosing personal email addresses (by using cc and not bcc);
- leaving a personnel file in a public area;
- losing your briefcase or personal device; and
- having your personal drive hacked or otherwise compromised

Investigation into Suspected Data Breaches

In the event that we become aware of a breach, or a potential breach, an investigation will be carried out. This investigation will be carried out by **Clare Hall College Bursar** who will make a decision over whether the breach is required to be notified to the Information Commissioner.

When a Breach will be Notified to the Information Commissioner

In accordance with the GDPR, we will undertake to notify the **Information Commissioner** of a breach which is likely to pose a risk to people's rights and freedoms. A risk to people's freedoms can include physical, material or non-material damage such as discrimination, identity theft or fraud, financial loss and damage to reputation.

Notification to the Information Commissioner will be done without undue delay and at the latest within 72 hours of discovery. If we are unable to report in full within this timescale, we will make an initial report to the Information Commissioner, and then provide a full report in more than one instalment if so required.

CLARE HALL
CAMBRIDGE

We will provide the following information:

a) a description of the nature of the personal data breach including, where possible:

   i) the categories and approximate number of individuals concerned; and
   ii) the categories and approximate number of personal data records concerned

b) the name and contact details of the **Clare Hall Data Protection Officer** and where more information can be obtained;
c) a description of the likely consequences of the personal data breach; and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

When an Individual Will be Notified of the Breach

In accordance with GDPR, we will undertake to notify the individual whose data is the subject of a breach if there is a *high* risk to people's rights and freedoms; for example, where there is an immediate threat of identity theft, or if special categories of data are disclosed online.

This notification will be made without undue delay and may, dependent on the circumstances, be made before the supervisory authority is notified.

The following information will be provided when a breach is notified to the affected individuals:

a) a description of the nature of the breach
b) the name and contact details of the **Clare Hall Data Protection Officer** and where more information can be obtained
c) a description of the likely consequences of the personal data breach and
d) a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Record of Breaches

Clare Hall records all personal data breaches regardless of whether they are notifiable or not as part of its general accountability requirement under GDPR.
It records the following information:

a) your contact details (for follow up enquiries if necessary);
b) the date of discovery, and the date of the incident (the two may be different…);
c) details about how the incident happened and how it was discovered;
d) the extent of the incident (i.e. how many personal records may have been affected, and what exposure there may be of different types of personal data);
e) the likely consequences for both the data subjects and the College.

A form to record all of this information has been developed.
You should ask for help and assistance from your Head of Department and/or the Colleges Data Protection Lead or, if they are unavailable from the Office of Intercollegiate Services (college.dpo@ois.cam.ac.uk).

CLARE HALL
CAMBRIDGE

IMPORTANT:
Personal data incidents may also be data (IT) security incidents. Where this is the case, you must complete the form noted above **and also** report the security incident by contacting the Computer Emergency Response Team at UIS (cert@cam.ac.uk).

Further information relating to Data Protection may be found on the Clare Hall GDPR Webpage at www.clarehall.cam.ac.uk.

Last updated: 09/06/18