DATA BREACH POLICY

SEPTEMBER 2020

CONTENTS

CONTENTS

INTRODUCTION

The General Data Protection Regulation (GDPR) aims to protect the rights of individuals about whom data is obtained, stored, processed or supplied and requires that organisations take appropriate security measures against unauthorised access, alteration, disclosure or destruction of personal data.

The GDPR places obligations on our College team to report actual or suspected data breaches and our procedure for dealing with breaches is set out below. All members of the team are required to familiarise themselves with its content and comply with the provisions contained in it. Training will be provided to enable all team members to carry out their obligations within this policy.

Data Processors will be provided with a copy of this policy and will be required to notify the College of any data breach without undue delay after becoming aware of the data breach. Failure to do so may result in a breach to the terms of the processing agreement.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the College Team Code of Conduct and associated policies, up to and including summary dismissal depending on the seriousness of the breach.

This policy does not form part of any individual's terms and conditions of employment with the College and is not intended to have contractual effect. Changes to data protection legislation will be monitored and further amendments may be required to this policy to remain compliant with legal obligations.

Please refer to the College's Data Protection Policy for details on how we handle the personal data of our students, parents, trustees, governors, suppliers, members of the College team and other third parties.

SCOPE

The College has several Creative Learning Studios (CLS) that provide appropriate, challenging, and meaningful study programmes, to increase employability skills. This policy relates to distance learning and e-safety across all aspects of the work of the College.

Any reference to 'College' in this policy means each of the above CLS'.

Any reference to the College 'team' in this policy means all staff and volunteers working at each of the above CLS'.

OUR VALUES

To be Respectful, Responsible, Safe and Kind, are at the core of our values. They are reflective of expected behaviours and set the foundation upon which the College builds its culture.

COMMUNICATION

This policy will be:

- Displayed on the College website
- Included as part of the induction pack for all new staff.

REVIEW AND MONITORING

The Board of Governors and the College Lead are responsible for overseeing, reviewing, and updating this policy, which will be reviewed annually.

We will monitor the effectiveness of this and all our policies and procedures and conduct a full review and update as appropriate.

Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the College and all data subjects.

The College team will be informed or any updates or amendments.

RELATED POLICIES

This policy should be read in conjunction with the following policies:

Data Protection

Data Retention

REGISTRATION WITH THE INFORMATION COMMISSIONER'S OFFICE

The College, as data controller shall be registered with the Information Commissioner's Office (ICO) under the 1998 Data Protection Act and this will be renewed annually. The information that will be required for notification includes:

- Name and address of data controller
- Nominated representative (if applicable).
- Description of the personal data being processed and the category of data subject to which they relate
- Description of the purpose(s) for which the data is/are being processed
- Description of any recipients to whom the data will be disclosed
- Names of any countries outside the EEA to which data is or will be transferred.

DEFINITIONS

Personal Data

Personal data is any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers we possess or can

reasonably access. This includes special category data and pseudonymised personal data but excludes anonymous us data or data that has had the identity of an individual permanently removed.

Personal data can be factual (for examples a name, email address, location, or date of birth) or an opinion about that person's actions or behaviour.

Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual.

Special Category Data

Previously termed "Sensitive Personal Data", Special Category Data is similar by definition and refers to data concerning an individual's racial or ethnic origin, political or religious beliefs, trade union membership, physical and mental health, sexuality, biometric or genetic data and personal data relating to criminal offences and convictions.

Personal Data Breach

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 or special category data transmitted, stored, or otherwise processed. Examples of a data breach could include the following (but are not exhaustive): -

- Loss or theft of data or equipment on which data is stored, for example loss of a laptop or a paper file (this includes accidental loss);
- Inappropriate access controls allowing unauthorised use;
- Equipment failure;
- Human error (for example sending an email or SMS to the wrong recipient);
- Unforeseen circumstances such as a fire or flood;
- Hacking, phishing, and other "blagging" attacks where information is obtained by deceiving whoever holds it.

Data Subject

Person to whom the personal data relates.

ICO

ICO is the Information Commissioner's Office, the UK's independent regulator for data protection and information.

RESPONSIBILITY

The Data Protection Officer (DPO) is responsible for overseeing this policy and developing data-related policies and guidelines. Responsibility for day to day compliance is delegated to the College Lead.

Please contact the DPO with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed.

Data Protection Officer: Lindsey Rhodes

Address: 71 Westholme close, Congleton, CW12 4FZ

Email: lindsey@projectinc.co.uk

Telephone: 07773776862

WHEN TO REPORT A DATA BREACH

The College must notify the ICO of a data breach where it is likely to result in a risk to the rights and freedoms of individuals. This means that the breach needs to be more than just losing personal data and if unaddressed the breach is likely to have a significant detrimental effect on individuals.

Examples of where the breach may have a significant effect includes: -

- potential or actual discrimination;
- potential or actual financial loss;
- potential or actual loss of confidentiality;
- risk to physical safety or reputation;
- exposure to identity theft (for example through the release of non-public identifiers such as passport details);
- the exposure of the private aspect of a person's life becoming known by others.

If the breach is likely to result in a high risk to the rights and freedoms of individuals, then the individuals must also be notified directly.

PROCEDURE

Reporting A Data Breach

If a team member or data processor know or suspect a personal data breach has occurred or may occur which meets the criteria above, you should: -

- contact and discuss with the DPO and College Lead
- Complete a data breach report on the College share-point.

Where appropriate, the team member should liaise with their CLS Lead about recording of the data breach. Breach reporting is encouraged throughout the College and team members are expected to seek advice if they are unsure as to whether the breach should be reported and/or could result in a risk to the rights and freedom of individuals. They can seek advice from the College Lead or the DPO.

Once reported, you should not take any further action in relation to the breach. In particular, you must not notify any affected individuals or regulators or investigate further. The College Lead will acknowledge receipt of the data breach report and take appropriate steps to deal with the report in collaboration with the DPO.

Reporting Data Protection Concerns

Prevention is always better than dealing with data protection as an after-thought. Data security concerns may arise at any time and we would encourage you to report any concerns (even if they don't meet the criteria of a data breach) that you may have to the College Lead or the DPO. This can help capture risks as they emerge, protect the College from data breaches and keep our processes up to date and effective.

Managing and Recording the Breach

On being notified of a suspected personal data breach, the College Lead will notify the DPO. Collectively they will take immediate steps to establish whether a personal data breach has in fact occurred. If so, they will take steps to:

- Where possible, contain the data breach;
- As far as possible, recover, rectify, or delete the data that has been lost, damaged, or disclosed;
- Assess and record the breach in the College's data breach register;
- Notify the ICO;
- Notify data subjects affected by the breach;
- Notify other appropriate parties to the breach;
- Take steps to prevent future breaches.

Notifying the ICO

The College Lead will notify the ICO when a personal data breach has occurred which is likely to result in a risk to the rights and freedoms of individuals.

This will be done without undue delay and, where possible, within 72 hours of becoming aware of the breach. The 72 hours deadline is applicable regardless of College holidays (I.e. it is not 72 working hours). If the College Lead / DPO are unsure of whether to report a breach, the assumption will be to report it.

The 'report a breach' page of the ICO website (https://ico.org.uk/for-organisations/report-a-breach/) details all the information that must be set out to the ICO. If all these details are not yet known, the College Lead / DPO will report as much as they can within the 72 hours.

As required, the DPO will set out:

- A description of the nature of the personal data breach including, where possible
- The categories and approximate number of individuals concerned
- The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned.

If all the above details are not yet known, the DPO will report as much as they can within 72 hours. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible.

Notifying Data Subjects

Where the data breach is likely to result in a high risk to the rights and freedoms of data subjects, the College Lead / DPO will notify the affected individuals without undue delay including the name and contact details of the DPO and ICO, the likely consequences of the data breach and the measures the College have (or intended) to take to address the breach.

When determining whether it is necessary to notify individuals directly of the breach, the College Lead will co-operate with and seek guidance from the DPO, the ICO and any other relevant authorities (such as the police).

If it would involve disproportionate effort to notify the data subjects directly (for example, by not having contact details of the affected individual) then the College will consider alternative means to make those affected aware (for example by making a statement on the College website).

Notifying Other Authorities

The College will need to consider whether other parties need to be notified of the breach. For example, but not limited to: -

- Insurers;
- Parents;
- Third parties (for example when they are also affected by the breach);
- Local authority;
- The police (for example if the breach involved theft of equipment or data)
- Banks
- Credit card companies.

Assessing the Breach

Once initial reporting procedures have been carried out, the College Lead / DPO will carry out all necessary investigations into the breach.

The College Lead / DPO will identify how the breach occurred and take immediate steps to stop or minimise further loss, destruction, or unauthorised disclosure of personal data. Ways to recover correct or delete data will be identified (for example notifying our insurers or the police if the breach involves stolen hardware or data).

Having dealt with containing the breach, the College Lead / DPO will consider the risks associated with the breach. These factors will help determine whether further steps need to be taken (for example notifying the ICO and/or data subjects as set out above). These factors include: -

- What type of data is involved and how sensitive it is;
- The volume of data affected;
- Who is affected by the breach (i.e. the categories and number of people involved);
- The likely consequences of the breach on affected data subjects following containment and whether further issues are likely to materialise;
- Are there any protections in place to secure the data (for example, encryption, password protection, pseudonymisation);
- What has happened to the data;
- What could the data tell a third party about the data subject;

- What are the likely consequences of the personal data breach on the College; and
- Any other wider consequences which may be applicable.

Preventing Future Breaches

Once the data breach has been dealt with, the College will consider its security processes with the aim of preventing further breaches. To do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;
- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether it is necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief trustees/management following the investigation.

Version Number	
SLT Member Responsible for This Policy	
Board Approval Date	
Date of Next Review	