Data Breach Policy

Policy Ref: TMP43v2

This policy will not discriminate either directly or indirectly against any individual on grounds of sex, race, ethnicity or national origin, gender, sexual orientation, marital status, religion or belief, age, disability, socioeconomic status, offending background or any other personal characteristic.

Prepared By	Jackie Manning,	**Reviewed By**	Martin Heaton
Job Title	Assistant Director, Designated Safeguarding Lead	**Job Title**	Director
Signed		**Signed**	
Date	**July 2020**	**Date**	**July 2020**

Record of Changes

Version	Issue Date	Changes	Initials
v1	July 2019	Initial issue	JM
v2	July 2020	General procedural review, references updated, formatting changes	JM

Date of Next Review: July 2021

Overview

TMP College's reputation and future growth are dependent on the way it manages and protects Personal Data.

As an organisation that collects and uses Personal Data, TMP College takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise.

TMP College's key concern in relation to any breach affecting Personal Data is to contain the breach and take appropriate action to minimise, as far as possible, any adverse impact on any individual affected.

TMP College has therefore implemented this Policy to ensure all College Personnel are aware of what a Personal Data breach is and how they should deal with it if it arises.

This Policy does not form part of any College Personnel's contract of employment and TMP College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

A full list of definitions is provided in Appendix 1.

About this Policy

This Policy explains how TMP College complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the ICO and the affected individuals.

The College has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how TMP College deals with and records Personal Data breaches.

Scope

This Policy applies to all TMP College Personnel who collect and/or use Personal Data relating to individuals.

It applies to all Personal Data stored electronically, in paper form, or otherwise.

What is a Personal Data Breach?

TMP College takes information security very seriously and the College has security measures against unlawful or unauthorised processing of Personal Data and against the accidental loss of, or damage to, Personal Data. TMP College has in place procedures and technologies to maintain the security of all Personal Data from the point of collection to the point of destruction.

Personal Data breach is defined very broadly and is effectively any failure to keep Personal Data secure, which leads to the accidental or unlawful loss (including loss of access to), destruction, alteration or unauthorised disclosure of Personal Data.

Whilst most Personal Data breaches happen as a result of action taken by a third party, they can also occur as a result of something someone internal does.

A Personal Data breach could include any of the following:

- loss or theft of Personal Data or equipment that stores Personal Data;
- loss or theft of Personal Data or equipment that stores TMP College's Personal Data from a College supplier;
- inappropriate access controls meaning unauthorised College Personnel can access Personal Data;
- any other unauthorised use of or access to Personal Data;
- deleting Personal Data in error;
- human error (which could be as simple as putting a letter in the wrong envelope or leaving a phone or laptop containing Personal Data on a train);
- hacking attack;
- infection by ransom ware or any other intrusion on our systems/network;
- 'blagging' offences where information is obtained by deceiving the organisation who holds it; or
- destruction or damage to the integrity or accuracy of Personal Data.

A Personal Data breach can also include:

- equipment or system failure that causes Personal Data to be temporarily unavailable;
- unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;
- inability to restore access to Personal Data, either on a temporary or permanent basis; or
- loss of a decryption key where Personal Data has been encrypted because this means the College cannot restore access to the Personal Data.

Reporting a Personal Data Breach

TMP College Personnel must immediately notify any Personal Data breach to the Data Protection Officer, no matter how big or small and whether or not College Personnel think a breach has occurred or is likely to occur. This allows the College to contain the breach as soon as possible and to consider a recovery plan to minimise any risk of damage to the individuals affected and to the College.

If TMP College Personnel discover a Personal Data breach outside working hours, College Personnel must notify it to the College's Data Protection Officer as soon as possible.

TMP College Personnel may be notified by a third party (e.g. a supplier that processes Personal Data on the College's behalf) that they have had a breach that affects College Personal Data. College

Personnel must notify this breach to the College's Data Protection Officer and the College's Data Breach Notification Procedure shall apply to the breach.

Managing a Personal Data Breach

There are four elements to managing a Personal Data breach or a potential one and this Policy considers each of these elements:

1. Containment and recovery
2. Assessment of on-going risk
3. Notification
4. Evaluation and response

At all stages of this Policy, the Data Protection Officer and managers will consider whether to seek external legal advice.

1. Containment and Recovery

An initial assessment of the Personal Data breach will be carried out by the Data Protection Officer.

If the Personal Data breach is unlikely to result in a risk to the rights and freedoms of the individuals affected then it will be added to the College's Data Breach Register and no further action will be taken.

If the Personal Data breach may impact on the rights and freedoms of the individuals affected then TMP College will put together and implement a bespoke Personal Data breach plan to address the breach concerned in accordance with the College's Data Breach Notification Procedure. This will include consideration of:

- whether there are any other people within TMP College who should be informed of the breach, such as IT team members, to ensure that the breach is contained;
- what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and
- whether it is necessary to contact other third parties such as learners, parents, banks, the ICO or the police particularly in the case of stolen Personal Data. All notifications shall be made by the Data Protection Officer.

All actions taken in relation to a Personal Data breach will be in accordance with the Data Breach Notification Procedure which is maintained and administered by the Data Protection Officer.

The Data Protection Officer is responsible for ensuring that the Data Breach Register is updated.

2. Assessment of Ongoing Risk

As part of TMP College's response to a Personal Data breach, once the breach has been contained the College will consider the on-going risks to the College and to any other party caused by the breach and what remedial action can be taken to minimise the impact of the breach. This will be undertaken in accordance with TMP College's Data Breach Notification Procedure.

3. Notification

Under Data Protection Laws, TMP College may have to notify the ICO and also possibly the individuals affected about the Personal Data breach.

Any notification will be made by the Data Protection Officer following TMP College's Data Breach Notification Procedure. The notification shall comply with the requirements of the ICO.

Notification of a Personal Data breach must be made to the ICO without undue delay and where feasible within 72 hours of when the College becomes aware of the breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. It is therefore imperative that College Personnel notify all Personal Data breaches to the College in accordance with the Data Breach Notification Procedure immediately.

Notification of a Personal Data breach must be made to the individuals affected without undue delay where the breach is likely to result in a high risk to the rights and freedoms of individuals.

Please note that not all Personal Data breaches are notifiable to the ICO and/or the individuals affected and the College will decide whether to notify and who to notify in accordance with the Data Breach Notification Procedure.

Where the Personal Data breach relates to a temporary loss of availability of TMP College's systems, the College does not have to notify if the lack of availability of Personal Data is unlikely to result in a risk to the rights and freedoms of individuals. The College does not consider that it has any systems where temporary unavailability would cause a risk to the rights and freedoms of individuals but this will be assessed on a case-by-case basis in accordance with the Data Breach Notification Procedure.

In the case of complex breaches, TMP College may need to carry out in-depth investigations. In these circumstances, TMP College will notify the ICO with the information that it has within 72 hours of awareness and will notify additional information in phases. Any delay in notifying the ICO must be seen as exceptional and shall be authorised in accordance with the Data Breach Notification Procedure.

Where a Personal Data breach has been notified to the ICO, any changes in circumstances or any relevant additional information which is discovered in relation to the Personal Data breach shall also be notified to the ICO in accordance with the Data Breach Notification Procedure.

When TMP College notifies the affected individuals, it will do so in clear and plain language and in a transparent way. Any notifications to individuals affected will be done in accordance with the Data Breach Notification Procedure. Any notification to an individual should include details of the action the College has taken in relation to containing the breach and protecting the individual. It should also give any advice about what they can do to protect themselves from adverse consequences arising from the breach.

TMP College may not be required to notify the affected individuals in certain circumstances as exemptions apply. Any decision whether to notify the individuals shall be done in accordance with the Data Breach Notification Procedure and shall be made by the Data Protection Officer.

4. Evaluation and Response

It is important not only to investigate the causes of the breach but to document the breach and evaluate the effectiveness of the College's response to it and the remedial action taken.

There will be an evaluation after any breach of the causes of the breach and the effectiveness of the College's response to it. All such investigations shall be carried out in accordance with the Data Breach Notification Procedure and will be recorded on the Personal Data Breach Register.

Any remedial action such as changes to TMP College's systems, policies or procedures will be implemented in accordance with the Data Breach Notification Procedure.

Appendix 1: Definitions

TMP College – TMP Studios CIC, 830 Ormskirk Road, Pemberton, Wigan, WN5 8EX

College Personnel – Any employee, worker or contractor who accesses any of TMP College's Personal Data and includes employees, consultants, contractors, subcontractors, agency staff or temporary staff hired to work on behalf of TMP College.

Controller – Any entity (e.g. company, organisation or person) that makes its own decisions about how it is going to collect and use Personal Data. A Controller is responsible for compliance with Data Protection Laws. TMP College acts as Controller in relation to areas such as the collection of employee details or enrolment information collected for its learners. It is the organisation itself which is the Controller not the staff.

Data Protection Laws – The General Data Protection Regulation (Regulation (EU) 2016/679) and all applicable laws relating to the collection and use of Personal Data and privacy and any applicable codes of practice issued by a regulator including in the UK, the Data Protection Act 2018.

Data Protection Officer – TMP College's Data Protection Officer is **Jackie Manning** and can be contacted via the main TMP College telephone number 01942 212607 or on email via jackiemanning@music-projects.com

ICO – the Information Commissioner's Office, the UK's data protection regulator.

Individuals – Living individuals who can be identified, directly or indirectly, from information that TMP College has. For example, an individual could be identified directly by name, or indirectly by gender, job role and office location if you can use this information to work out who they are. Individuals include employees, learners, parents, visitors and potential learners. Individuals also include our partners and employers.

Personal Data – Any information about an Individual (see definition above) which identifies them or allows them to be identified in conjunction with other information that is held. It includes information of this type, even if used in a business context. Personal data is defined broadly and covers things such as name, address, email address (including in a business context, email addresses of Individuals in companies such as firstname.surname@organisation.com), IP address and also more sensitive types of data such as trade union membership, health data, genetic data and religious beliefs. These more sensitive types of data are called "Special Categories of Personal Data" and are defined below. Special Categories of Personal Data are given extra protection by Data Protection Laws.

Processor – Any entity (e.g. company, organisation or person) which accesses or uses Personal Data on the instruction of a Controller. A Processor is a third party that processes Personal Data on behalf of a Controller. This is usually as a result of the outsourcing of a service by the Controller or the provision of services by the Processor which involve access to or use of Personal Data. College examples include, software support we receive for our college learner record system, which contains

Personal Data, and outsourcing delivery of learning where we define the purpose and the processing requirements involved.

Special Categories of Personal Data – Personal Data that reveals a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data (i.e. information about their inherited or acquired genetic characteristics), biometric data (i.e. information about their physical, physiological or behavioural characteristics such as facial images and fingerprints), physical or mental health (including learning difficulties or disabilities), sexual life or sexual orientation and criminal convictions. Special Categories of Personal Data are subject to additional controls in comparison to ordinary Personal Data.