Data Breach Policy 2023-24

1 Overview Information

Lead Responsible:	Data Protection Officer
Approval Dates for Revisions:	
Equality Impact Assessment	
Audit Committee	2 March 2023
Governing Body	29 March 2023
Effective Date:	30 March 2023
Annual Review Date:	Spring 2024
Original Filename:	Z:\Data Protection\Policies-Process\Current Policies\Draft Data Breach Policy 2023-24.docx

Overview

1.1. The College's reputation and future growth are dependent on the way the College manages and protects Personal Data. As an organisation that collects and uses Personal Data, the College takes seriously its obligations to keep that Personal Data secure and to deal with security breaches relating to Personal Data when they arise. The 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. The College has therefore implemented this Policy to ensure all College Personnel are aware of what a Personal Data breach is and the necessary steps that need to be taken if such a breach occurs.

1.2. College Personnel will receive a copy of this Policy when they start and may receive periodic revisions of this Policy. This Policy does not form part of any College Personnel's contract of employment and the College reserves the right to change this Policy at any time. All College Personnel are obliged to comply with this Policy at all times.

About this policy

1.3. This Policy explains how the College complies with its obligations to recognise and deal with Personal Data breaches and (where necessary) to notify the Information Commissioner's Office (ICO) and the affected individuals. The College has a corresponding Data Breach Notification Procedure and Data Breach Register that set out how the College deals with and records Personal Data breaches.

1.4. **Note: Please refer to the accompanying template Data Breach Notification and Internal Data Breach Register.**

Scope

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

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

Definitions

1.7. **College** – Capel Manor College, located at five sites across the Greater London area (Bullsmoor Lane, Crystal Park, Gunnersbury Park, Regent's Park and Brooks Farm).

1.8. **College Personnel** – Any College employee or contractor who has been authorised to access any of the College's Personal Data and will include employees, consultants, contractors, and temporary personnel hired to work on behalf of the College.

1.9. **Data Protection Laws** – The UK General Data Protection Regulation (Regulation (UK GDPR) 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.

1.10. **Data Protection Officer** – The Data Protection Officer is Richard Davies and can be contacted at: dataprotection@capel.ac.uk

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

1.12. **Personal Data** – any information about an individual which identifies them or allows them to be identified in conjunction with other information that is held. Personal data is defined very broadly and covers both ordinary personal data from personal contact details and business contact details to special categories of personal data such as trade union membership, genetic data and religious beliefs. It also covers information that allows an individual to be identified indirectly for example an identification number, location data or an online identifier.

1.13. **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, sexual life or sexual orientation and criminal record.

What is a personal data breach

1.14. The 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. The 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.

1.15. Personal Data breach is defined very broadly and, in summary, is 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 the correct procedures not being followed by College staff.

1.16. A Personal Data breach could include any of the following:

1.16.1. loss or theft of Personal Data or equipment that stores Personal Data;

1.16.2. loss or theft of Personal Data or equipment that stores the College's Personal Data from a College supplier;

1.16.3. inappropriate access controls meaning unauthorised College Personnel can access Personal Data;

1.16.4. any other unauthorised use of or access to Personal Data;

1.16.5. deleting Personal Data in error;

1.16.6. 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);

1.16.7. malicious computer hacking attack;

1.16.8. infection by ransom ware or any other intrusion on College systems / network;

1.16.9. 'blagging' offences where information is obtained by deceiving the organisation who holds it; or

1.16.10. destruction or damage to the integrity or accuracy of Personal Data.

1.17. A Personal Data breach can also include:

1.17.1. equipment or system failure that causes Personal Data to be temporarily unavailable;

1.17.2. unforeseen circumstances such as a fire, flood or power failure that causes Personal Data to be temporarily unavailable;

1.17.3. inability to restore access to Personal Data, either on a temporary or permanent basis; or

1.17.4. 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

1.18. College staff must immediately notify any potential or suspected Personal Data breach to the Data Protection Officer, no matter how big or small. 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.

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

1.20. College staff 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

1.21. There are four elements to managing a Personal Data breach:

1.21.1. Containment and recovery

1.21.2. Assignment of on-going risk

1.21.3. Notification

1.21.4. Evaluation and response

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

Containment and recovery

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

1.24. 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.

1.25. If the Personal Data breach may impact on the rights and freedoms of the individuals affected then the 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:

1.25.1. whether there are any other people within the College who should be informed of the breach, such as IT team members, to ensure that the breach is contained;

1.25.2. what steps can be taken to contain the breach, recover the loss of any Personal Data or to prevent damage being caused; and

1.25.3. whether it is necessary to contact other third parties such as students, 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.

1.26. 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.

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

Assessment of ongoing risks

1.28. As part of the 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 the College's Data Breach Notification Procedure.

Notification

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

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

1.31. 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.

1.32. 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.

1.33. 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.

1.34. Where the Personal Data breach relates to a temporary loss of availability of the 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.

1.35. In the case of complex breaches, the College may need to carry out in-depth investigations. In these circumstances, the 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.

1.36. 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.

1.37. When the 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.

1.38. The 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.

Evaluation and response

1.39. 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.

1.40. 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.

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