1 8 9 3 Writtle University College

Data Breach Notification Policy

Writtle University College
Lordship Road, Chelmsford
Essex, CM1 3RR

Tel: +44 (0)1245 424200
Fax: +44 (0)1245 420456
Email: info@writtle.ac.uk
www.writtle.ac.uk

Policy Owner	Department
Data Protection Officer	Professional Support
Version Number	**Date drafted/Date of review**
1.1	22 February 2019
Date Equality Impact Assessed	**Has Prevent been considered (see Policies Guidance if unsure)**
25 May 2018	Yes
Reviewed and Approved by (see Policies Guidance for approval process)	**Date**
SLT Governors	4 July 2018 13 July 2018
Access (tick as appropriate)	
Public access (website) ☒ And/Or Internal access (MyWi) ☒	Staff and Student access ☒ Or Staff access only ☐

Policy Overview and Scope

Writtle University College ("WUC") collects, holds, processes and shares personal data and considers this data as a valuable asset which needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidental or deliberate) to avoid a data protection breach which could compromise security.

This policy applies to all staff and students at WUC. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of WUC.

Policy and Procedure

1. Definitions and Types of Breach

1.1 For the purposes of this Policy, data security breaches include both confirmed and suspected incidents.

1.2 A data security breach is defined very broadly and 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.

1.3 A data security breach could include, but is not restricted to, any of the following:

1.3.1 loss or theft of personal data or equipment that stores personal data (e.g. loss of laptop, USB stick, iPad / tablet or paper record or file);

1.3.2 unauthorised use of, access to or modification of data or information systems;

1.3.3 deleting personal data in error;

1.3.4 attempts (failed or successful) to gain unauthorised access to information or IT systems);

1.3.5 unauthorised disclosure of personal data;

1.3.6 human error (e.g. putting a letter in the wrong envelope or sending to the wrong postal or email address or leaving a phone or laptop containing personal data on a train)

1.3.7 hacking attack;

1.3.8 infection by ransom ware or any other intrusion on our systems or network;

1.3.9 'blagging' offences where information is obtained by deceiving the organisation who holds it;

2. Reporting an Incident

2.1 Any individual who accesses, uses or manages WUC's information is responsible for reporting a data breach immediately to the Data Protection Officer (dpo@writtle.ac.uk) or 01245 424200.

2.2 If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable.

2.3 The report must include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved.

3. Managing a Data Security Breach

3.1 There are four elements to managing a data security breach and these are considered in full below:

3.1.1 Containment and recovery

3.1.2 Assessment of on-going risk

3.1.3 Notification

3.1.4 Evaluation and response

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

4. Containment and Recovery

4.1 The Data Protection Officer (DPO) will firstly determine if the breach is still occurring. If so, the appropriate steps will be taken immediately to minimise the effect of the breach.

4.2 An initial assessment will be made by the DPO in liaison with the relevant officer(s) to establish the severity of the breach and decide who will take the lead in investigating the breach as the Lead Investigation Officer (LIO). This will depend on the nature of the breach: in some cases it will be the DPO.

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

4.4 If the breach may impact on the rights and freedoms of the individuals affected then the University College will put together and implement a bespoke Data Breach Plan to address the breach. This will include consideration of:

4.4.1 whether there are any other people within the University College who should be informed of the breach, such as IS team members, to ensure the breach is contained;

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

4.4.3 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.

4.5 The DPO is responsible for ensuring that the Data Breach Register is updated.

5. Assessment of Ongoing Risk

5.1 Once the breach has been contained, an investigation will be undertaken by the DPO with the LIO and other relevant officers.

5.2 Any ongoing risks to the institution or to any other party will be considered together with remedial action that can be taken to minimise the impact of the breach.

5.3 The investigation will take into account the following:

- The type of data involved;
- Its sensitivity;
- The protections in place (e.g. encryption);
- What has happened to the data (e.g. has it been lost or stolen);
- Whether the data could be put to any illegal or inappropriate use;
- Data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- Whether there are wider consequences of the breach.

6. Notification

6.1 The DPO, in consultation with relevant colleagues and the Senior Leadership Team, will establish whether the Information Commissioner's Office (ICO) will need to be notified of the breach. If yes, the notification must be made within 72 hours of becoming aware of the breach, where feasible.

6.2 Every incident will need to be assessed on a case by case basis, however, the following will need to be considered:

6.2.1 whether the breach is likely to result in a high risk of adverse effect to an individual's rights and freedoms;

6.2.2 whether notification would assist the individual(s) affected (e.g. could they act on the information to mitigate risks?)

6.2.3 whether notification would help prevent the unauthorised or unlawful use of personal data;

6.2.4 whether there are any legal/contractual notification requirements;

6.2.5 the dangers of over notifying. Not every incident warrants notification and over notification may cause disproportionate enquiries and work.

6.3 Individuals whose personal data has been affected by the incident, and where it has been considered likely to result in a high risk of adverse effect to their rights and freedoms, will be informed without undue delay.

6.4 A record will be kept of any personal data breach on the Data Breach Register, regardless of whether notification was required.

6.5 The Data Breach Register will be reviewed by the Senior Leadership Team and Audit Committee of Governors on an annual basis. Audit Committee will also be made aware as soon as reasonably practicable of any breaches which are notified to the ICO.

7. Evaluation and Response

7.1 Once the initial incident is contained, the DPO will carry out a full review of the cause of the breach and the effectiveness of the response and whether any changes to systems, policies and procedures should be undertaken to minimise the risk of similar incidents occurring.

8. Additional Guidance and Related Policies

8.1 For further guidance and advice, please contact the Data Protection Officer – dpo@writtle.ac.uk. Alternatively, visit the Information Commissioner’s Website - https://ico.org.uk/.

8.2 Related policies:

- Data Protection Policy
- IS&T Policy

This policy supersedes any other policy and procedural guidelines, which may be in other existing University College documents. Writtle University College may amend this policy from time to time and any such amendments will be notified via the website, MyWi or by email.

If this information is difficult to access, read or understand, it can be provided in another format, for example in large print, or by someone talking it through with you.

Version Control

Version Number	Purpose/Amendment	Date
1.0	New policy - GDPR	25 May 2018
1.1	Minor changes for DPO	22 February 2019