Breach Policy and Procedure

Formal Review Cycle:	**Annual**		
Latest Formal Review (month/year):	**2018-04**	Next Formal Review Due (month/year):	**2019-04**
Policy Owner:	**Data Protection Officer**		
Impact Assessed by:	**JS**	Impact Assessment Date:	**2018-03**

APPROVAL REQUIRED:

SMT Y/N	**Y**	SMT Date approved:	**2018-04-23**		
Governor Y/N	**Y**	Committee:	**Board**	Governor Date approved:	**17-05-2018**

PUBLICATION:

Website Y/N	**Y**	Intranet Y/N	**Y**	Student VLE Y/N	**Y**	Other:	
Area/s of Staff Intranet:	**IT; MIS; DPO**						

Contents

Personal data breach notification policy

1. Introduction

1.1 Data security breaches are increasingly common occurrences whether these are caused through human error or via malicious intent. As technology trends change and the creation of data and information grows, there are more emerging ways by which data can be breached. The College must have in place a robust and systematic process for responding to any reported data security breach to ensure that it can act responsibly and protect its information assets as far as possible. It must also be able to quickly establish the type of breach and whether other authorities must be notified.

1.2 This policy sets out the policies and procedures of *Craven College* (the "College") with respect to detection of personal data breaches, responding to personal data breaches and notification of personal data breaches to supervisory authorities, data controllers and data subjects. When dealing with personal data breaches, the College and all College personnel must focus on protecting individuals and their personal data, as well as protecting the interests of the College.

1.3 The aim of this policy is to standardise the College-wide response to any reported data breach incident, and ensure that they are appropriately logged and managed in accordance with best practice guidelines.

By adopting a standardised consistent approach to all reported incidents it aims to ensure that:

- incidents are reported in a timely manner and can be properly investigated;
- incidents are handled by appropriately authorised and skilled personnel;
- appropriate levels of College management are involved in response management;
- incidents are recorded and documented;
- the impact of the incidents is understood and action is taken to prevent further damage;
- evidence is gathered, recorded and maintained in a form that will withstand internal and external scrutiny;
- external bodies or data subjects are informed as required;
- the incidents are dealt with in a timely manner and normal operations restored; and
- the incidents are reviewed to identify improvements in policies and procedures.

1.4 Staff, students, contractors, consultants, visitors and guests who act in breach of this policy, or who do not act to implement it, may be subject to disciplinary procedures or other appropriate sanctions.

2. Definitions

2.1 In this policy:

(a) "**appointed person**" means the individual primarily responsible for dealing with personal data breaches affecting the College, being the Data Protection Officer of the College;

(b) "**data controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;

(c) "**data processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(d) "**data subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

(e) "**personal data**" means any information relating to a data subject;

(f) "**personal data breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the College (including any temporary or permanent loss of control of, or inability to access, personal data);

(g) "**data security breach**" is considered to be any loss of, or unauthorized access to, College data. Examples of data security breaches include:

- Loss or theft of data or equipment on which data is stored;
- Unauthorised access to confidential or highly confidential College Data;
- Equipment failure;
- Human error;
- Unforeseen circumstances such as a fire or flood;
- Hacking attack;
- 'Blagging' offences where information is obtained by deceit.

For the purposes of this policy data security breaches include both confirmed and suspected incidents; and

(h) "**supervisory authority**" means the Information Commissioner's Office of the United Kingdom.

3. Scope

3.1 This College-wide policy applies to all College information, regardless of format, and is applicable to all staff, students, visitors, contractors and data processors acting on behalf of the College. It is to be read in conjunction with the College Information Security Policy and the General Data Protection Policy and replaces the former Data Loss Reporting Policy.

4. Responsibilities

4.1 Information users - **All** information users are responsible for reporting actual, suspected, threatened or potential information security incidents and for assisting with investigations as required, particularly if urgent action must be taken to prevent further damage.

4.2 Heads of School/Department - Heads of Departments and School are responsible for ensuring that staff in their area act in compliance with this policy and assist with investigations as required.

4.3 Lead Responsible Officers - Lead responsible officers will be responsible for overseeing management of the breach in accordance with the Data Breach Management Plan. Suitable delegation may be appropriate in some circumstances.

4.4 Contact Details - In the event that the Incident Management Team need to be contacted, please contact the IT Helpdesk on 01756 693839, located in the Ingleborough Building on the Aireville Campus.

5. Data Classification

5.1 Data security breaches will vary in impact and risk depending on the content and the quantity of the data involved, therefore it is important that the College is able to quickly identify the classification of the data and respond to all reported incidents in a timely and thorough manner.

5.2 All reported incidents will need to include the appropriate data classification in order for assessment of risk to be conducted. Data classification referred to in this policy means the following approved College Data Categories:

- ***Public Data*** - Information intended for public use, or information which can be made public without any negative impact for the College.
- ***Internal Data*** - Information regarding the day-to-day business and academic operations of the College. Primarily for staff and student use, though some information may be useful to third parties who work with the College.
- ***Confidential Data*** - Information of a more sensitive nature for the business and academic operations of the College, representing the basic intellectual capital and knowledge. Access should be limited to only those people that need to know as part of their role within the College.
- ***Highly confidential Data*** - Information that, if released, will cause significant damage to the College's business activities or reputation, or would lead to breach of the Data Protection Act / General Data Protection Regulation. Access to this information should be highly restricted.
- ***Personal data*** **-** any information relating to a data subject.

6. Responding to personal data breaches

6.1 All personnel of the College must notify the appointed person, the Data Protection Officer (DPO), immediately if they become aware of any actual or possible personal data breach. The DPO can be reached on the following email address: dpo@craven-college.ac.uk , and, contact the IT Helpdesk on: helpdesk@craven-college.ac.uk or on 01756 693839. Where possible the incident report form, in Appendix 1, should be completed as part of the reporting process.

6.2 The Data Protection Officer (DPO) is primarily responsible for investigating possible and actual data breaches and for determining whether they involve personal data and if any notification obligations apply. Once a data breach has been reported an initial assessment will be made to establish the severity of the breach and who the lead responsible officer to lead should be as per Appendix 2. All data security breaches will be centrally logged in the IT Helpdesk System to ensure appropriate oversight in the types and frequency of confirmed incidents for management and reporting purposes. Where notification obligations apply, the appointed person is responsible for notifying the relevant third parties in accordance with this policy.

6.3 All personnel of the College must cooperate with the appointed person in relation to the investigation and notification of personal data breaches.

6.4 The appointed person must determine whether the College is acting as a data controller and/or a data processor with respect to each category of personal data that is subject to a personal data breach.

6.5 The steps to be taken by the appointed person when responding to a personal data breach may include:

(a) ensuring that the personal data breach is contained as soon as possible;
(b) assessing the level of risk to data subjects as soon as possible;
(c) gathering and collating information from all relevant sources;
(d) considering relevant data protection impact assessments;

(e) informing all interested persons within the College of the personal data breach and the investigation, including *the Principal and other relevant members of the SMT*;
(f) assessing the level of risk to the College; and
(g) notifying supervisory authorities, data controllers, data subjects and others of the breach in accordance with this policy.

6.6 The appointed person shall keep a full record of the response of the College to a personal data breach, including the facts relating to the personal data breach, its effects and the remedial action taken. This record shall form part of the personal data breach register of the College.

7. Data Breach Management Plan

7.1 The management response to any reported data security breach will involve the following four elements. See Appendix 3 for suggested checklist.

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

7.2 Each of these four elements will need to be conducted in accordance with the checklist for Data Security Breaches. An activity log recording the timeline of the incident management should also be completed. See Appendix 4.

8. Notification to supervisory authority

8.1 This section 8 applies to personal data breaches affecting personal data with respect to which the College is acting as a data controller.

8.2 The College must notify the supervisory authority of any personal data breach to which this section 8 applies without undue delay and, where feasible, not later than 72 hours after the College becomes aware of the breach, save as set out in subsection 8.4.

8.3 Personal data breach notifications to the supervisory authority must be made by the appointed person using the form set out in Appendix 5 (Notification of personal data breach to supervisory authority). The completed form must be sent to the supervisory authority by secure and confidential means. The appointed person must keep a record of all notifications, and all other communications with the supervisory authority relating to the breach, as part of the personal data breach register of the College.

8.4 The College will not notify the supervisory authority of a personal data breach where it is unlikely to result in a risk to the rights and freedoms of natural persons. The appointed person shall be responsible for determining whether this subsection 8.4 applies, and the appointed person must create a record of any decision not to notify the supervisory authority. This record should include the appointed person's reasons for believing that the breach is unlikely to result in a risk to the rights and freedoms of natural person. This record shall be stored as part of the personal data breach register of the College.

8.5 To the extent that the College is not able to provide to the supervisory authority all the information specified in Appendix 5 (Notification of personal data breach to supervisory authority) at the time of the initial notification to the supervisory authority, the College must make all reasonable efforts to ascertain the missing information. That information must be provided to the supervisory authority, by the appointed person, as and when it

becomes available. The appointed person must create a record of the reasons for any delayed notification under this subsection 8.5. This record shall be stored as part of the personal data breach register of the College.

8.6 The College must keep the supervisory authority informed of changes in the facts ascertained by the College which affect any notification made under this section 8.

9. Notification to data controller/processor

9.1 The College recognises that although it is not required to notify a processor in the event of a breach, it accepts that under some circumstances the DPO would need to contact processors of data for which the College is a controller.

9.2 This section 9 applies to personal data breaches affecting personal data with respect to which the College is acting as a data controller.

9.3 The College must notify the affected data controller(s) of any personal data breach to which this section 9 applies without undue delay and, where feasible, not later than 72 hours after the College becomes aware of the breach. In addition, the College must comply with the provisions of the contract(s) with the affected data controller(s) relating to such notifications.

9.4 Personal data breach notifications to the affected data controller(s) must be made by the appointed person using the form set out in Appendix 6 (Notification of personal data breach to data controller). The completed form must be sent to the affected data controller(s) by secure and confidential means. The appointed person must keep a record of all notifications, and all other communications with the affected data controller(s) relating to the breach, as part of the personal data breach register of the College.

9.5 To the extent that the College is not able to provide to the affected data controller(s) all the information specified in Appendix 6 (Notification of personal data breach to data controller) at the time of the initial notification to the affected data controller(s), the College must make all reasonable efforts to ascertain the missing information. That information must be provided to the affected data controller(s), by the appointed person, as and when it becomes available.

10. Notification to data subjects

10.1 This section 10 applies to personal data breaches affecting personal data with respect to which the College is acting as a data controller.

10.2 Notifications to data subject under this section 10 should, where appropriate, be made in consultation with the supervisory authority and in accordance with any guidance given by the supervisory authority with respect to such notifications.

10.3 The College must notify the affected data subjects of any personal data breach to which this section 10 applies if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, save as set out in subsection 10.5.

10.4 Personal data breach notifications to the affected data subjects must be made by the appointed person in clear and plain language using the form set out in Appendix 7 (Notification of personal data breach to data subject). The completed form must be sent to the affected data subjects by appropriate means. The appointed person must keep a record of all notifications, and all other communications with the affected data subjects relating to the breach, as part of the personal data breach register of the College.

10.5 The College has no obligation to notify the affected data subject of a personal data breach if:

(a) the College has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption), and those measures have been applied to the personal data affected by the personal data breach;

(b) the College has taken subsequent measures which ensure that a high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) it would involve disproportionate effort (in which case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner),

providing that the appointed person shall be responsible for determining whether this subsection 10.5 applies, and the appointed person must create a record of any decision not to notify the affected data subjects. This record should include the appointed person's reasons for believing that the breach does not need to be notified to the affected data subjects. This record shall be stored as part of the personal data breach register of the College.

10.6 If the College is not required by this section 10 to notify affected data subjects of a personal data breach, the College may nonetheless do so where such notification is in the interests of the College and/or the affected data subjects.

11. Other notifications

11.1 Without affecting the notification obligations set out elsewhere in this policy, the appointed person should also consider whether to notify any other third parties of a personal data breach. Notifications may be required under law or contract. Relevant third parties may include:

(a) the police;
(b) other law enforcement agencies;
(c) insurance companies;
(d) professional bodies;
(e) regulatory authorities;
(f) financial institutions; and/or
(g) trade unions or other employee representatives.

12. Reviewing and updating this policy

12.1 The Data Protection Officer shall be responsible for reviewing and updating this policy.

12.2 This policy must be reviewed and, if appropriate, updated annually.

12.3 This policy must also be reviewed and updated on an *ad hoc* basis if reasonably necessary to ensure:

- the compliance of the College with applicable law, codes of conduct or industry best practice;
- the security of data stored and processed by the College; or
- the protection of the reputation of the College.

12.4 The following matters must be considered as part of each review of this policy:

- changes to the legal and regulatory environment;
- changes to any codes of conduct to which the College subscribes;
- developments in industry best practice;

- any new data collected by the College;
- any new data processing activities undertaken by the College; and
- any security incidents affecting the College.

Breach Policy and Procedure

Appendix 1: Data Breach Incident Report Form

Description of the Data Breach:	
Time and Date breach was identified and by whom.	
Who is reporting the breach: Name/Post/Dept.	
Contact details: Telephone/Email	
Classification of data breached (more than one may apply): 1. Public Data 2. Internal Data 3. Confidential Data 4. Highly confidential Data 5. Personal Data	
Volume of data involved	
Confirmed or suspected breach?	
Is the breach contained or ongoing?	
If ongoing, what actions are being taken to recover the data?	
Who has been informed of the breach?	
Any other relevant information?	

Email form immediately to the Data Protection Officer: dpo@craven-college.ac.uk and the IT Helpdesk: helpdesk@craven-college.ac.uk and/or call the IT helpdesk on 01756 693839 and advise the engineers that a Data Security Breach report form is being sent.

For office us only:

Received by:	
Date/Time:	
DPO informed: (inc. date and time)	
IT Manager informed: (inc. date and time)	

Breach Policy and Procedure

Appendix 2: Evaluation of Data Breach Incident Severity

The severity of the incident will be assessed per the standard IS Incident Management Process (by the Data Protection Officer and the IS Service Management team during office hours OR the IS Duty Incident Manager outside office hours). Assessment would be made based upon the following criteria:

High Criticality: Major Incident	Contact:
• Highly Confidential/Confidential Data • Personal data breach involves > 1000 individuals • External third party data involved • Significant or irreversible consequences • Likely media coverage • Immediate response required regardless of whether it is contained or not • Requires significant response beyond normal operating procedures	Lead Responsible Officer: • Data Protection Officer: dpo@craven-college.ac.uk • On call Duty Principal (if out of hours) Other relevant contacts: • Governance and Information Compliance • Internal senior managers as required • Contact external parties as required i.e. police/ICO/individuals impacted
Moderate Criticality: Serious Incident	**Contact:**
• Confidential Data • Not contained within College • Breach involves personal data of more than 100 individuals • Significant inconvenience will be experienced by individuals impacted • Incident may not yet be contained • Incident does not require immediate response • Incident response may require notification	Lead Responsible officer: • Head of School or Department affected by the incident, or • On call Duty Principal (if out of hours) Other relevant contacts: • Data Protection Officer • Technology Services Department Manager • Facilities Manager • Director of Human Resources • Marketing Manager • Senior Management
Low Criticality: Minor Incident	**Contact:**
• Internal or Confidential Data • Small number of individuals involved • Risk to College low • Inconvenience may be suffered by individuals impacted • Loss of data is contained/encrypted • Incident can be responded to during working hours Example: • Email sent to wrong recipient • Loss of encrypted mobile device	Lead Responsible Officer: • Head of School/Faculty or Department (May delegate responsibility to another appropriate senior member of staff) Other relevant contacts: • Data Protection Officer • Technology Services Department Manager • Facilities Manager

Breach Policy and Procedure

Appendix 3: Data Breach Checklists

A. Containment and Recovery
B. Assessment of Risks
C. Consideration of Further Notification
D. Evaluation and Response

Step	Action	Notes
A	Containment and Recovery:	To contain any breach, to limit further damage as far as possible and to seek to recover any lost data.
1	• Data Protection Officer and/or • Technology Services Department Manager to ascertain the severity of the breach and determine if any personal data is involved.	See Appendix 2
2	• Data Protection Officer and/or • Technology Services Department Manager to identify Lead Responsible Officer for investigating breach and forward a copy of the data breach report	To oversee full investigation and produce report. Ensure lead has appropriate resources including sufficient time and authority. In the event that the breach is severe, the College Incident Management Team will be contacted to lead the initial response.
3	Identify the cause of the breach and whether the breach has been contained? Ensure that any possibility of further data loss is removed or mitigated as far as possible	Establish what steps can or need to be taken to contain the breach from further data loss. Contact all relevant departments who may be able to assist in this process. This may involve actions such as taking systems offline or restricting access to systems to a very small number of staff until more is known about the incident.
4	Determine whether anything can be done to recover any losses and limit any damage that may be caused	E.g. physical recovery of data/equipment, or where data corrupted, through use of back-ups.
5	Where appropriate, the Lead Responsible Officer or nominee to inform the police.	E.g. stolen property, fraudulent activity, offence under Computer Misuse Act.
6	Ensure all key actions and decisions are logged and recorded on the timeline.	
B	**Assessment of Risks**	**To identify and assess the ongoing risks that may be associated with the breach.**
7	What type and volume of data is involved?	Data Classification/volume of individual data etc.

8	How sensitive is the data?	Sensitive personal data? By virtue of definition within the General Data Protection Regulation (GDPR) (e.g. health record) or sensitive because of what might happen if misused (banking details).
9	What has happened to the data?	E.g. if data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.
10	If the data was lost/stolen, were there any protections in place to prevent access/misuse?	E.g. encryption of data/device.
11	If the data was damaged/corrupted /lost, were there protections in place to mitigate the impact of the loss?	E.g. back-up tapes/copies.
12	How many individuals' personal data are affected by breach?	
13	Who are the data subjects/individuals whose data has been compromised?	Students, applicants, staff, customers, clients or suppliers?
14	What could the data tell a third party about the individual? Could it be misused?	Consider this regardless of what has happened to the data. Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people.
15	Is there actual/potential harm that could come to any individuals?	E.g. are there risks to: • physical safety; • emotional wellbeing; • reputation; • finances; • identify (theft/fraud from release of non-public identifiers); • or a combination of these and other private aspects of their life?
16	Are there wider consequences to consider?	E.g. a risk to public health or loss of public confidence in an important service we provide?
17	Are there others who might advise on risks/courses of action?	E.g. If individuals' bank details have been lost, consider contacting the banks themselves for advice on anything they can do to help you prevent fraudulent use.

C	Consideration of Further Notification	Notification is to enable individuals who may have been affected to take steps to protect themselves or allow the regulatory bodies to perform their functions.
18	Are there any legal, contractual or regulatory requirements to notify?	E.g.: terms of funding; contractual obligations
19	Can notification help the College meet its security obligations under the seventh data protection principle?	E.g. prevent any unauthorised access, use or damage to the information or loss of it.
20	Can notification help the individual?	Could individuals act on the information provided to mitigate risks (e.g. by changing a password or monitoring their account)?
21	If a large number of people are affected, or there are very serious consequences, inform the Information Commissioner's Office (through the Data Protection Officer).	Contact and liaise with the Data Protection Officer if not already involved. Where a reportable breach has occurred under GDPR the College has only 72 hours to inform the ICO.
22	Consider the dangers of 'over notifying'.	Not every incident will warrant notification "and notifying a whole 2 million strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work".
23	Consider whom to notify, what you will tell them and how you will communicate the message.	• There are a number of different ways to notify those affected so consider using the most appropriate one. Always bear in mind the security of the medium as well as the urgency of the situation. • Include a description of how and when the breach occurred and what data was involved. Include details of what has already been done to respond to the risks posed by the breach. • When notifying individuals give specific and clear advice on the steps they can take to protect themselves and also what the institution is willing to do to help them. • Provide a way in which they can contact us for further information or to ask questions about what has occurred (e.g. a contact name, helpline number or a web page).
24	Consult the ICO guidance on when and how to notify it about breaches.	Where there is little risk that individuals would suffer significant detriment, there is no need to report. There should be a presumption to report to the ICO where a

		large volume of personal data is concerned and there is a real risk of individuals suffering some harm. Cases must be considered on their own merits and there is no precise rule as to what constitutes a large volume of personal data. Guidance available from https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/
25	Consider, as necessary, the need to notify any third parties who can assist in helping or mitigating the impact on individuals.	E.g. police, insurers, professional bodies, funders, trade unions, website/system owners, bank/credit card companies.
D	**Evaluation and Response**	**To evaluate the effectiveness of the College's response to the breach.**
26	Establish where any present or future risks lie.	
27	Consider the data and contexts involved.	E.g. what data is held, its extent, sensitivity, where and how it is stored, how long it is kept.
28	Consider and identify any weak points in existing security measures and procedures. Revisit the Data Impact Assessments and ensure they are fit for purpose.	E.g. in relation to methods of storage and/or transmission, use of storage devices, levels of access, systems/network protections.
29	Consider and identify any weak points in levels of security awareness/training.	Fill any gaps through training or tailored advice.
30	Report on findings and implement recommendations.	Report to Audit Committee.

Appendix 4: Timeline of Incident Management

Date	Time	Activity	Decision	Authority

Breach Policy and Procedure
APPENDIX 5: (NOTIFICATION OF PERSONAL DATA BREACH TO SUPERVISORY AUTHORITY)

1. Introduction

This personal data breach notification is made by Craven College, having its registered office at *Aireville Campus, Gargrave Road, Skipton, N. Yorks, BD23 1US.*

2. Description of personal data breach

[Describe circumstances of personal data breach, including date and time when data controller became aware of the breach]

3. Categories of data subject affected

[Specify categories of data subject affected]

4. Number of data subjects affected

[Insert number or approximate number of data subjects affected]

5. Categories of personal data concerned

[Specify categories of personal data concerned]

6. Number of records concerned

[Insert number or approximate number of records concerned]

7. Likely consequences of breach

[Identify likely consequences of breach]

8. Measures taken to address breach

[Describe measures taken to address breach]

9. Has breach been notified to data subjects?

The breach [has] OR [has not] been notified to affected data subjects. The reason for not notifying affected data subjects is *[specify reason]*.

10. Late report of breach

The breach is being reported more than 72 hours after the data controller became aware of the breach because *[give reasons]*.

11. Contact details

The name of the person responsible for handling the breach is *[insert name]*, and [his] OR [her] contact details are as follows: *[insert contact details]*.

Breach Policy and Procedure
APPENDIX 6: (NOTIFICATION OF PERSONAL DATA BREACH TO DATA CONTROLLER/PROCESSOR)

1. Introduction

This personal data breach notification is made by Craven College, having its registered office at *Aireville Campus, Gargrave Road, Skipton, N. Yorks, BD23 1US.*

2. Description of personal data breach

[Describe circumstances of personal data breach, including date and time when data controller became aware of the breach]

3. Categories of data subject affected

[Specify categories of data subject affected]

4. Number of data subjects affected

[Insert number or approximate number of data subjects affected]

5. Categories of personal data concerned

[Specify categories of personal data concerned]

6. Number of records concerned

[Insert number or approximate number of records concerned]

7. Likely consequences of breach

[Identify likely consequences of breach]

8. Measures taken to address breach

[Describe measures taken to address breach]

9. Contact details

The name of the person responsible for handling the breach is *[insert name]*, and [his] OR [her] contact details are as follows: *[insert contact details]*.

Breach Policy and Procedure
APPENDIX 7: (NOTIFICATION OF PERSONAL DATA BREACH TO DATA SUBJECT)

1. Introduction

This personal data breach notification is made by Craven College, having its registered office at *Aireville Campus, Gargrave Road, Skipton, N. Yorks, BD23 1US.*

2. Description of personal data breach

[Describe circumstances of personal data breach, including date and time when data controller became aware of the breach]

3. Categories of personal data concerned

[Specify categories of personal data concerned]

4. Likely consequences of breach

[Identify likely consequences of breach]

5. Measures taken to address breach

[Describe measures taken to address breach]

6. Steps to mitigate breach

[Insert details of steps data subject may take to mitigate personal data breach]

7. Contact details

The name of the person responsible for handling the breach is *[insert name]*, and [his] OR [her] contact details are as follows: *[insert contact details]*.