Data Protection Policy

Formal Review Cycle:	**Annual**		
Latest Formal Review (month/year):	**2017-04**	Next Formal Review Due (month/year):	**2018-04**
Policy Owner:	**R BROOKE**		
Impact Assessed by:	**MW**	Impact Assessment Date:	**2013-05-17**

APPROVAL REQUIRED

SMT Y/N	**Y**	SMT Date approved:	**2016-09-21**		
Governor Y/N	**Y**	Committee:	**Audit**	Governor Date approved:	**2017-05-02**

PUBLICATION

Website Y/N	**Y**	Intranet Y/N	**Y**	Student VLE Y/N	**Y**	Other:	
Area/s of Staff Intranet:	**MIS, Human Resources**						

Policy description:

This policy is intended to define the policy and principles adopted by Craven College (College) to govern the processing of personal data as specified in the Data Protection Act 1998. Management and staff must have an awareness of the obligations imposed by the Act and, depending on the nature of the information being stored or processed, take appropriate steps to ensure that the College complies with the legislation.

Through its day to day operations the College is required to collect and hold certain types of information about individuals. These include learners, customers, suppliers, current, past and prospective employees, volunteers and others with whom it communicates. In addition, it may occasionally be required by law to collect and use certain types of information of this kind to comply with the requirements of government departments. The Data Protection Act includes safeguards to ensure personal information is dealt with properly regardless of how it is collected, recorded and used, whether on paper, electronic or other medium.

Supporting documentation:

- DPA Disclosure Guidelines
- DPA Registration

Links to other policies:

- Technology Services - Acceptable IT Use Policy
- Technology Services – Technology Strategy 2015 – 2018
- Human Resources – Confidentiality and Copyright Policy
- College Safeguarding Policy
- Staff Code of Conduct
- Social and Electronic Media Policy
- Health and Safety Policy

Contents

1. Legislative Framework

The current Data Protection Act was introduced in 1998. "The Act" is intended to protect the rights of individuals whose personal data is stored and processed by organisations and establishments.
The 1998 Data Protection Act defines data as any information which:

- is processed using equipment operating automatically in response to instructions
- is recorded with the intention of being processed
- is recorded as part of a relevant filing system
- forms part of an accessible record, including health records

Data Protection under the 1998 Act is about ensuring that personal data about an individual is processed fairly and lawfully in order to protect the rights of an individual.

2. Definitions of Personal and Sensitive Data

- All identifiable individuals' information
- All identifiable staff information
- Any other identifiable information held on any other person, whether held in electronic or paper form

Certain types of data are regarded as sensitive, and "the Act" stipulates that special measures must be taken in the processing and protection of this type of data.
Sensitive data includes:

- Racial or ethnic origins
- Political opinions
- Religious or similar beliefs
- Membership of trade union
- Physical or mental health condition
- Sexual life
- Any proceedings for any offence or criminal convictions

3. Policy Statement

The College regards the lawful and correct treatment of personal data as crucial to the successful delivery of the highest quality of service. The lawful and correct processing of personal information is a key part of building trust and confidence with external and internal customers. Therefore-

- The College will fully implement all aspects of the Data Protection Act 1998.
- The College will ensure all staff and other individuals are fully aware of both their rights and obligations under "the Act".
- The College will implement adequate and appropriate physical and technical security measures and organisational measures to ensure the security of all information contained in or handled by those systems, including computer systems.
- It is not the College's policy to transfer individual's data and the College will only transfer personal data outside the European Economic Area (EEA) if the explicit consent of the individual concerned has been given.

4. Aims of Policy

The aims of the policy are to fully deliver the Principles as stated in the Data Protection Act 1998.

First Principle:
Personal data shall be processed fairly and lawfully, and in particular, shall not be processed unless specific conditions are met.

Second Principle:
Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that or those purposes.

Third Principle:
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Fourth Principle:
Personal data shall be accurate and where necessary, kept up to date.

Fifth Principle:
Personal data shall not be kept longer than necessary, for that purpose or those purposes.

Sixth Principle:
Personal data shall be processed in accordance with the rights of the data subjects in this Act.

Seventh Principle:
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss destruction of, or damage to, personal data.

Eighth Principle:
Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5. Scope of Policy

The policy covers all aspects of the College's business relating to personal information. The policy covers all methods of holding and storing information including:

- manually stored paper data, e.g. application and enrolment records, personnel records etc.
- data held in computer applications and databases
- data from CCTV and other audio or visual recording systems
- data held in archive storage
- data held on CD ROMs, floppy disks, computer disks, memory sticks, mobile electronic devices etc.

6. Practical Implications

Conformance with the Data Protection Act is part of the College's duty of confidentiality towards learners, customers, staff and other individuals with whom it deals. As general guidance the terms of the Act mean that all managers and staff have a responsibility to ensure compliance with the Act and this policy and also to develop and encourage good information handling practices, within their areas of responsibility. All users of personal data within the

College have a responsibility to ensure that they process the data in accordance with the eight Principles and the other conditions set down in the DPA.

In particular they will:

- ensure that information is collected, processed, held, transferred and disposed of appropriately, with care for its quality and security
- ensure that the rights of people about whom information is held can be fully exercised under the DPA, including the right to access information

In addition, the College will ensure that:

- staff understand their responsibilities with respect to the proper handling of data through the management, supervision, and training
- there is someone with specific responsibility for data protection in the organisation
- anybody wanting to make enquiries about handling personal information knows what to do and enquiries are dealt with promptly and courteously
- the requirements of the DPA are considered in processes, such as in the development of policy and procedures and the design and the implementation of information systems and the monitoring and evaluation of operational systems and performance

In order to meet the requirements of the principles, the College will:

- observe fully the conditions regarding the fair collection and use of personal data
- meet its obligations to specify the purposes for which personal data is used
- collect and process appropriate personal data only to the extent that it is needed to fulfil operational or any legal requirements
- ensure the quality of personal data used
- apply checks to determine the length of time personal data is held;
- ensure that the rights of individuals about whom the personal data is held, can be fully exercised under the Act
- take the appropriate technical and organisational security measures to safeguard personal data
- ensure that personal data is not transferred abroad without suitable safeguards
- ensure that all contracts with third parties are data protection compliant

7. Responsibilities of Management, Staff and Students

This section of the Policy identifies the Data Protection responsibilities of various members of staff and students.

GOVERNING BODY

The Governing Body is committed to, and ultimately responsible for, ensuring that the College establishes and adheres to policies and procedures which are compliant with the law and best practice and will therefore approve all policies relating to data protection in the College. The SMT and Data Protection Officer will ensure that the Board of Governors is aware of any issues arising from the policy and procedures.

SMT

The Senior Management team is responsible for ensuring that the College is fully compliant with the law and best practice for handling personal information. SMT will:

- Approve College policies & procedures for handling personal information.
- Review developments in good practice and Codes of Practice issued by the Information Commissioner having a bearing on College activities, updating College policies and procedures, as appropriate.

- Allocate resources to enable the Data Protection Policy to be practically and proactively applied within the College.
- Ensure that the College's information strategy is matched to its business needs and that the appropriate links are made between Data Protection, IT Security, Information Security, Records Management and Freedom of Information and that a co-ordinated approach to these issues is adopted and maintained.

DATA PROTECTION OFFICER

The Data Protection Officer is responsible for maintaining the College's Data Protection systems. The Data Protection Officer will:

- Maintain the College's Data Protection Notification.
- Investigate any potential issues surrounding Data Protection and report findings to SMT.
- Liaise with the Information Commissioner and respond to assessments.
- Make recommendations to SMT regarding Data Protection Policy and good practice.
- Provide general guidance and advice and dissemination of information regarding Data Protection.
- Deal with subject access requests and co-ordinate responses to complaints.
- Co-ordinate and advise on all non-routine requests for disclosure of personal information.
- Monitor and report on compliance.

MANAGERS

Good personal data handling is one aspect of delivering excellent customer service. The key to achieving high standards in handling personal information is recognising that the primary responsibility for complying with legislation and good practice lies with the staff who are responsible for deciding how the personal information is used. Managers of each area of the College will:

- Ensure they are satisfied with the legality of holding and using the information.
- Ensure that the use of personal data complies with all appropriate College policies.
- Ensure that the staff they manage receive appropriate Data Protection training.
- Refer any non-routine requests for disclosure, requests for subject access and requests to cease processing to the Data Protection Officer immediately.

IT SERVICES

All staff and users of personal data have some responsibility for the security of that data. IT Staff have an important role in ensuring the security of computerised data. In particular they will:

- Be responsible for advising the College on the state of technological development with regard to IT security.
- Back up data on the College's IT systems.
- Implement virus detection and hacking preventative measures.
- Under instruction from SMT or the Data Protection Officer, place appropriate restrictions on access so that individuals only have access to personal data in which they have a legitimate business interest.
- Require the use of passwords and ensure they are changed regularly.
- Promote policies for the use of College IT facilities including email, intranet and internet.
- Investigate breaches of IT security.

H R

An important aspect of security is ensuring the reliability of staff. Human Resources can contribute to this in a number of ways. They will:-

- Ensure that the College's Employment Practices are consistent with the Employment Practices Code of Practice.
- Ensure that Data Protection obligations are reflected in the College's Disciplinary Procedures and contracts of employment.
- Ensure that all staff are aware of the types of personal information that the College will routinely make public (eg name, post, qualifications, telephone or email) and that individuals have the right to object to that disclosure when they consider it may cause them substantial damage or distress.
- Ensure that all obligations outlined within the DBS Code of Practice published under section 122 of the Police Act 1997 are adhered to. Full details of the DBS Code of Practice can be found at http://www.homeoffice.gov.uk/dbs/.
- Provide advice to managers and others on the application of the DBS Code of Practice.

OTHER STAFF

All staff are likely to have access to some personal information in the course of their duties. They will:-

- Respect the privacy and confidentiality rights of all data subjects.
- Be careful that personal information is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party. This includes making sure that casual access to data is not possible on screen or otherwise.
- Only use personal information for approved purposes and ensure that they comply with any instructions and guidelines about the use of personal data.
- Inform the Data Protection Officer of any proposed new uses of personal data.
- Keep all personal data secure and not remove it from college premises without the permission of their line manager.
- Comply with all College policies regarding the use of IT facilities.
- Check that the information they provide to the College in connection with their employment is accurate and up-to-date and inform the College of changes to or errors in information held.

STUDENTS

Students will not normally process personal data on behalf of the College. However, from time to time there may be circumstances where this happens and it is the responsibility of the tutor to ensure that guidelines are followed appropriately. For periods of work experience within the college, the student should be considered a member of staff and therefore must be made aware of their rights and responsibilities within the appropriate sections above. It is the responsibility of the work experience supervisor to ensure that this process is followed and they should also be prepared to limit access to information where they feel it is inappropriate in a given circumstance.

At all times students will:-

- Respect the privacy and confidentiality rights of all data subjects.
- Not seek to gain unauthorised access to personal information.
- Comply with all College policies regarding the use of IT facilities.
- Check that the information they provide to the College in connection with their studies is accurate and up-to-date and inform the College of changes to or errors in information held.

8. Disclosure of information to external organisations/parties.

The College collects a wide range of personal data relating to staff and students for its own purposes, and to meet external obligations. This may result in the eventual transfer of personal data to an outside third party, however any such transfers must be permitted under the Act.

- Personal data must not be disclosed to unauthorised third parties. Unauthorised third parties includes another individual or organisation, family members, friends, local authorities, government bodies, and the police where the individual has not consented to the transfer unless disclosure is exempted by the 1998 Act, or by other legislation. There is no general legal requirement to disclose information to the police.

However data can sometimes be disclosed without consent, where, for example, it is required for:

- protecting the vital interests of the data subject (i.e. release of medical data in emergency)
- the prevention or detection of crime

Transferring information to another third party, with the data subjects consent.
Personal Data can be transferred to another third party if the data subject has given their consent. This must always be in writing.

Consent cannot be inferred from silence, so if the College requests consent so that personal data can be provided to a third party, and no response is received, the College must infer that consent is withheld.

Disclosure of information to a sponsor or prospective employers
A further issue arises where sponsors or prospective employers contact the College to verify details about a student, such as attendance records and examination results. In most circumstances, students would not object to the disclosure of such information, and indeed it would appear to benefit the student. However, best practice suggests that the request for information should be accompanied by a statement from the student consenting to the disclosure, or at least that the student should be contacted to confirm their consent.

Providing information because it is required by law
The College is frequently required to disclose information in accordance with legislation which it is subject to, eg the College is required to provide information to the Inland Revenue regarding employees' salaries.

Data Security during Transit
Every effort should be made to ensure that any data being transferred, regardless of whether electronic or otherwise, remains secure.

- Personal data should be sent via a tracked postal service ie. recorded delivery.
- Any electronically stored personal data must be password protected, and where possible encrypted, with the password being sent to the recipient via alternative means. This includes floppy disk, CD, DVD, memory stick, memory cards, laptops, PDA's, email etc.
- The originating member of staff should confirm safe receipt of the information from the recipient and highlight any potential losses to the Data Protection Officer immediately.

9. Data Subject Rights

Right of subject access
Staff, learners and other users of the College have the right to access any personal data that is being kept about them either on computer or in certain files. Any person who wishes to exercise this right should complete the College Subject Access Request Form (Appendix 1). All formal requests using the Subject Access Request Form are recorded by the Data Protection Officer to monitor compliance with the Act.

The College is able to make a change of £10 per data request.

The College aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days. In cases of unavoidable delay, the reason for delay will be explained in writing to the data subject making the request.

Right to prevent processing likely to cause unwarranted damage or distress
A data subject is entitled to request in writing that the College does not process personal data where such processing is likely to cause unwarranted damage or distress to him/her. This right does not apply where:-

- The data subject has given consent previously to the processing or the processing is necessary for the purposes of fulfilling a contract with the data subject, fulfilling a legal obligation of the College or for protecting the data subject's vital interests.

Right to prevent direct marketing
A data subject is entitled at any time to request in writing that the College does not process personal data for the purposes of direct marketing.

Rights in relation to automated decision making
Subject to certain exemptions, a data subject is entitled at any time, in writing, to require that the College ensures no decision which significantly affects him/her is based **solely** on the processing of personal data by automatic means. Where a decision which significantly affects the data subject is based solely on such automatic processing, the College must notify him/her that the decision was taken on that basis. Any human intervention in an automated process is deemed to show that the decision is not solely automatic. A data subject is entitled to request to be told the logic behind any automated decision making process.

Rights to compensation
Where a data subject suffers damage or damage and distress as a result of the breach of any of the requirements of the Act, he/she may apply to the Courts for compensation.

Compensation for distress alone can only be claimed where the College breaches any requirements of the Act when processing his/her personal data in relation to journalistic, artistic or literary purposes.

Rights to request rectification, blocking, erasure and destruction of inaccurate data
A data subject may apply to the Court for an order requiring the College to rectify, block, erase or destroy data relating to him/her if they are inaccurate.

A data subject may request that the Information Commissioner assesses whether or not it is likely that any processing of personal data has been or is being carried out by the College in

non-compliance with the Act. Depending on the Commissioner's assessment, Information Notices may be served or the Commissioner may take enforcement action.

10. ROLES AND RESPONSIBILITIES

All Staff
Staff at all levels within the College have a responsibility to actively respond to any concerns relating to confidentiality, and ensuring that personal information is processed in accordance with the rights of the individual.

Reporting of Data Protection Incidents
The notification process detailed in Appendix 1 should be adhered to when Data Protection Incidents are identified.

Principal
The Principal has overall responsibility for the implementation and delivery of this Data Protection Policy on behalf of College's Governing Board.

The Data Protection Officer
The Data Protection Officer on behalf of the Principal is responsible for facilitating the implementation of the policy and supporting the College's staff to understand their responsibilities.

The Data Protection Officer on behalf of the Principal also has responsibility for ensuring that the College is fully compliant with the rules for notification including:

- that a notification is lodged in its name with the Information Commissioner
- that the notification is lodged within the stipulated time period
- that the notification is concise, correct and maintained
- that any changes are notified within the stipulated time period
- fee notification

Managers, Heads of Departments and Line Managers
All managers, heads of departments and line managers have a responsibility to understand the Act and other related guidance, to establish appropriate procedures to control and manage information and ensure these procedures are followed in compliance with the Data Protection Act 1998.

11. Policy Review
This policy will be reviewed annually or in response to legislative changes.

12. Contact Details
In you have any general enquiries regarding Data Protection please contact:

Internal
Robert Brooke
The Data Protection Officer
Craven College

Information Commissioner's Office
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

http://ico.org.uk/for_organisations/data_protection

13. Glossary of Terms

Data
Data is information which is processed by a computer or manually held which forms part of a relevant filing system. A relevant filing system is a system that is structured either by reference to an individual or by criteria relating to individuals so that specific details relating to a particular individual may be easily selected from that system. Data can be written information, photographs or information like fingerprints, voice recordings, etc. From 2005 the definition of data under the Freedom of Information Act extends to include unstructured manual data but there are transitional arrangements for Data Protection which allow the existing definition of relevant filing systems to stand for existing systems until 2007.

Personal Data
Personal data is information that relates to a living individual who can be identified from that data and other information in or likely to come into the possession of the Data Controller.

Sensitive Personal Data
Sensitive personal data is personal data of the following specific nature: racial or ethnic origin; political opinions; religious beliefs or beliefs of a similar nature; membership of Trade Unions; physical or mental health or condition; sexual life; commission or alleged commission of any offence; proceeding of any offence committed or alleged, the disposal of such proceedings or the sentence of the court.

Processing
Processing is anything done with the data including holding and viewing it. If you have personal data you should assume you are processing it.

Implicit consent
The data subject may be asked to agree implicitly to the disclosure of information about themselves to certain named third parties. In the case of a student this consent is given when they sign an enrolment form or agree to the terms via an online process. In the case of staff this is implicitly given by signing the contract.

Explicit consent
Where sensitive personal data is to be disclosed to a third party, explicit consent must be sought from the data subject before the disclosure can take place. This consent is for the named disclosure and cannot be taken as consent for other or further processing of the data in this way. It needs to be collected each time such a disclosure is to be made.

Data Subject
The Data Subject is the individual who is the subject of personal data. This will include staff, students, suppliers of goods, visitors, contractors, etc.

Data Controller
The Data Controller is the legal person or body who determines the purposes for which and the manner in which any personal data are, or are to be, processed. The College is the Data Controller.

Data Processor
The Data Processor is any person other than an employee of the Data Controller who processes data on behalf of the Data Controller

Third Party
A Third Party is any person other than the Data Subject, the Data Controller, the Data processor or other person authorised to process data for the Data Controller.

DBS
Disclosure & Barring Service (http://www.homeoffice.gov.uk/dbs)

Appendix 1 to the Data Protection Policy : Standard Request Form for Access to Data

Craven College
Subject Access Request Form

The Data Protection Act 1998 gives students, staff and other users of the College the right to access personal data relating to themselves that is held by the College as part of a 'relevant filing system' (both in electronic and manual format). Any individual who wishes to access data should apply using this Subject Access Request Form.

The College needs to be assured of the applicant's identity before relevant data is released and a fee (£10.00) is due when a request for the release of data is made. Please note that the College may require a period of 40 days in which to provide the required information.

1) ARE YOU THE DATA SUBJECT?

Yes – are you applying for data the College holds about you? You will need to supply the College with evidence of your identity (student/staff ID card, proof of address, driving licence, birth certificate (or photocopy) etc.) as well as a signed copy of this form. This is to ensure we only release data to those who have a right to see the information.

Now complete Q2, 4 and 5

No - are you acting on behalf of the Data Subject with their written authority? If so, you will need to enclose an original copy of their permission to disclose. This can be a letter which is signed personally by them giving you authority. We must be able to confirm from our records that this request relates to the Data Subject. You will be the applicant. The Data Subject details must be included at Q3.

Now complete Q 2, 3, 4 and 5

2) DETAILS OF APPLICANT

Surname: **Former Surname (if applicable):**	**First Names:**

Address (Including postcode):	**Telephone (day):** **Telephone (eve):** **Mobile:**

3a) Details of the Data Subject (if different to 2)

Full Name: _____

Address: _____

Telephone Number: _____ **Fax Number:** _____

Email address: _____

3b) Please describe your relationship with the Data Subject that leads you to make this request on their behalf

_____

_____

_____

Complete 4 a/b/c as appropriate

4a) STUDENTS

Are you a present or past student of this College? **Yes/No** **Present/Past**

If yes, please give your course of study (and your current year, if applicable)

_____

_____

For past students, provide course title and dates of study:

_____

_____

4b) STAFF

4c) OTHERS (neither staff nor student)

If neither staff nor student please provide details of your connection with the College:

_____

_____

5) INFORMATION SOUGHT/REQUIRED

The College may hold personal records in different parts of its organisation. Please be specific if there is particular information you require and identify where you think this information will be held:

_____

_____

_____

_____

_____

Declaration

I……., certify that the information given on this application form to Craven College is true. I understand that it is necessary for Craven College to confirm my identity and it may be necessary to obtain more detailed Information in order to locate the correct information.

Signed:…….

Date:……..

Please return the form to Data Protection Officer, MIS Department, Craven College, Skipton, North Yorkshire, BD23 1US. Documents which must accompany this application are:

1. evidence of your identity
2. evidence of the Data Subject's identity (if different from above)
3. evidence of Data Subject's consent to disclose to a third party (if required as indicated above)
4. a fee of £10 (cheques to be made payable to Craven College)
5. stamped addressed envelope for return of proof of identity/authority documents,
6. where appropriate

Please note that the College reserves the right to obscure or suppress information that relates to other third parties (under the terms of Section 7 of the Data Protection Act 1998)