

## DATA PROTECTION POLICY

**Prepared by:** Marketing & Learner Services Manager

**Policy Approved by:** Strategic Management Team 20/10/2009 Minute 1739  
01/03/2011 Minute 1930  
Data protection group 06/04/2011 Minute 28  
Corporation 07/12/2009 Minute 727 (ii)  
05/07/2011 Minute 781 (i)

**Equality impact assessed & endorsed** 03/02/2011

**Last Reviewed** May 2001, June 2005, February 2007, October 2009, October 2010

**Review Date:** June 2012

## **Preamble to the Policy**

### **Equal Opportunities**

The College shall comply with all statutory duties in respect of equal opportunities in the areas of sex, race, age, disability, sexual orientation, transgender, religion, belief, pregnancy, maternity and paternity, marriage and civil partnership and the rehabilitation of offenders. The College shall also comply with the Human Rights Act 1998 and any subsequent enactments or modifications.

#### **1. Introduction**

- 1.1 The College needs to collect and keep certain data about its employees, learners and other users to allow it to exercise its function effectively. This includes monitoring its performance, organise learning provision, record learners' achievements, and maintain financial, health and safety and employment records.
- 1.2 Under certain condition of some financial grants, the College needs to share data with other public sector organisations. Staff and learners will be informed of when this could happen and the steps taken to ensure that no personal data that could identify the individual is transferred and when personal data is required specific consent is received.
- 1.3 The College collects data to meet its obligations to funding bodies and ensure government (and for example European) rules are complied with in respect of funding, e.g. to support financial audit requirements (see 1.2 above). Data collected also supports the process of staff recruitment and to facilitate payment of salaries and in some instances the payment of learner grants.
- 1.4 This policy aims to mitigate the risk to the security of data. Data is mainly obtained and processed from individuals and organisations mainly in College Functional Departments that include Learner Services, HR, Management Information Systems, Campus Services and Finance.
- 1.5 The College also collect data via CCTV system to enable it to perform its function in respect health and safety and prevention of crime
- 1.6 The College will do its utmost to ensure that the data collected is used fairly, stored safely and not disclosed to any other person unlawfully (see exception 1.2 above). Data will be destroyed safely when the duration that the data is held for it to comply with the law expires.
- 1.7 The College must comply with the Data Protection Principles that are set out in the Data Protection Act 1998 (the 1998 Act). In summary these state that personal data shall:
  - a) Be obtained and processed fairly and lawfully and shall not be processed unless certain conditions are met.

- b) Be obtained for a specified and lawful purpose and shall not be processed in any manner incompatible with that purpose.
  - c) Be adequate, relevant and not excessive for those purposes.
  - d) Be accurate and kept up to date.
  - e) Not be kept for longer than is necessary for that purpose.
  - f) Be processed in accordance with the data subject's rights.
  - g) Be kept safe from unauthorised access, accidental loss or destruction.
  - h) Not be transferred to a country outside the EU, unless that country has equivalent levels of protection for personal data.
- 1.8 The College and all staff or others who process or use any personal information must ensure that they follow these principles at all times. In order to ensure that this happens, the College has developed this Data Protection Policy.
- 1.9 The Freedom of Information Act 2000 gives a general right of access to all recorded information held by public authorities. However, this Act also sets out exemptions to that right and such exemptions include individual information on staff and learners by virtue of being personal information.

## **2. Status of the Policy**

- 2.1 This policy does not form part of the formal contract of employment, but it is a condition of employment that employees will abide by the rules and policies made by the College from time to time. Any failures to follow the policy can therefore result in disciplinary proceedings.
- 2.2 Any member of staff, who considers that the policy has not been followed in respect of personal data about him/her, should raise the matter with the designated data controller initially. If the matter is not resolved it should be raised as a formal grievance.

## **3. Notification of Data Held and Processed**

All staff, learners and other users are entitled to know

- what information the College holds and processes about them and why
- how to gain access to it,
- how to keep it up to date and
- what the College is doing to comply with its obligations under the 1998 Act.

The College will therefore provide all staff and learners and other relevant users with a standard form of notification. This will state all the types of data the College holds and processes about them, and the reasons for which it is processed. Management will, as part of the Employment Contract Process, seek specific consent from employees to process data relating to them.

#### **4. Responsibilities of Staff**

All staff are responsible for:

- 4.1.1 Checking that any information that they provide to the College in connection with their employment is accurate and up to date and informing the College of any changes to information, which they have provided e.g. changes of address.
- 4.1.2 Checking the accuracy of the information the College sends out from time to time, giving details of information kept and processed about staff.
- 4.1.3 Informing the College of any errors or changes. The College cannot be held responsible for any errors unless the staff member has informed the College of them.
- 4.1.4 If, and when, as part of their responsibilities, staff collect information about other people. (e.g. learners' personal details, data relating to learners' course work, opinions about ability, references to other academic institutions, or details of personal circumstances), they must comply with the guidelines for staff, which are at appendix 1.
- 4.1.5 Notifying their line manager (who subsequently should inform the Principal/Chief Executive) of any suspected or actual breaches in data security that may lead to data loss relating to staff, learners or organisations.

#### **5. Data Security**

All staff are responsible for ensuring that any personal data they hold (for example of learners, staff or other organisations) is kept securely and that personal information is not disclosed either orally or in writing, electronically, or accidentally or otherwise to any unauthorised third party.

Some organisations that operate within the public sector (e.g. Careers Wales) have a legal status as a private company. Any request for data from such external organisations must be made in writing and requests referred to the Executive's Office so that it can be registered and approved by the Data Protection Officer

Staff should note that unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct.

Staff who are in contact with learners should ensure that screen savers are enacted if machines are left unattended. Furthermore to avoid the risk of personal data being accessed or displayed by any unauthorised person all computers should enact the 'password sign-on' routine should any computer not be used for 15 minutes for support Staff and 30 minutes for academic staff.

Personal information should be kept in a locked filing cabinet, or in a locked drawer, or if it is computerised, be password protected, or kept only on disk or pen-drives which should also be kept securely. Electronic data on all portable devices should be encrypted. Staff should seek technical advice from IT Dept. if they are unfamiliar with such processes.

Staff should NOT remove personal data relating to other staff, organisations or learners from College premises. This includes data kept on disk drives, electronic transmission to their home or other venues even if the data is to be used for work purposes.

The College will do its utmost to protect personal data held electronically-digitally on its computers and servers, this includes ensuring that all security software and other technical protection is enacted to diminish the risk of access to data, including remotely (e.g. via the internet).

The College will notify the ICO of any breach of security and management of held data. In the event that a breach has occurred the College shall implement its Breach Management Plan (Refer to Appendix 2 and also the Business Contingency Plan).

## **6. Learner Obligations**

Learners must ensure that all personal data provided to the College is accurate and up to date. They must ensure that change of address etc is notified to their course tutor. Learners who use the College computer facilities may, from time to time, process personal data. If they do they must notify a data controller.

## **7. Rights to Access Information**

- 7.1. 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 write directly to the Executive Office.
- 7.2. In order to gain access, an individual may wish to receive notification of the information currently being held. This request should be made in writing to the Executive Office.
- 7.3. The College has the right to make a charge and will review this periodically.
- 7.4. The College aims to comply with requests for personal information as quickly as possible, but will ensure that it is provided within the 40 days allowed by the Act.

## **8. Publication of College Information**

- 8.1. Information that is already in the public domain is exempt from the 1998 Act. It is College policy to make as much information public as possible, and in particular the following information may be available to the public for inspection: - names of members of the Corporation, list of staff and agendas, reports and Minutes of meetings of Corporation and its committees on request from the Governance Unit.

- 8.2. The internal phone list will not be a public document.
- 8.3. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact the relevant designated data controller (see Annex 1).

## **9. Subject Consent**

- 9.1. In many cases, the College can only process personal data with the consent of the individual. In some cases, if the data is sensitive, express consent must be obtained. Agreement to the College processing some specified classes of personal data is a condition of acceptance of a learner onto any course, and a condition of employment for staff. This includes information about previous criminal convictions.
- 9.2. Some jobs or courses will bring the applicants into contact with children of 16 and 18. The College has a duty under the Children's Act and other enactments to ensure that staffs are suitable for the job, and learners for the courses offered. The College also has a duty of care to all staff and learners and must therefore make sure that employees and those who use the College's facilities do not pose a threat or danger to other users.
- 9.3. The College will also ask for information about particular health needs, such as allergies to certain forms of medication, or any conditions such as asthma or diabetes. The College will only use the information in the protection of the health and safety of the individual, but will need consent to process in the event of a medical emergency, for example.

## **10. Processing Sensitive Information**

- 10.1. Sometimes it is necessary to process information about a person's health, criminal convictions, race and gender and family details. This may be to ensure the College is a safe place for everyone, or to operate other College policies such as the sick pay policy or equal opportunities policy. Because this information is considered sensitive, and it is recognised that the processing of it may cause particular concern or distress to individuals, staff and learners will be asked to give express consent for the College to do this. Offers of employment or course places may be withdrawn if an individual refuses to give consent to this without good reason. More information about this is available from the Head of HR for staff and Head of Learner Services or Curriculum Area Managers for learners.

## **11. The Data Controller and the Designated Data Controllers**

- 11.1. The College as a body corporate is the Data Controller under the Act, and the Corporation Board is therefore ultimately responsible for implementation. However, the designated data controllers will deal with day-to-day matters.

- 11.2. The College has a number of designated data controllers. They include the Head of HR, the Head of Learner Services, Data Management Manager, Assistant Estates Manager, Campus Service Managers and Curriculum Director representative (see appendix 3)
- 11.3. The College also has a number of authorised staff in academic areas to manage and deal with sensitive data relating to learners.

## **12. Examination Results**

- 12.1 Learners will be entitled to information about their results for both coursework and examinations. However, this may take longer than other information to provide. The College may withhold certificates, accreditation or references in the event that the full course fees have not been paid, or all books and equipment returned to the College.

## **13. Retention and Destruction of Data**

- 13.1 The College will keep some forms of data for longer than others. Because of storage problems, information about learners cannot be kept indefinitely, unless there are specific requests to do so. In general, information about learners will be kept for a maximum of 7 years after they leave the College. However it may be case that some data will have to be retained for a longer period to meet data retention requirements of such funding bodies as the EU. This will include name and address, academic achievements, including marks for coursework and copies of any reference written and name of employer.
- 13.2 All other information, including any information about health, race or disciplinary matters will be destroyed within a shorter period of the course ending and the learner leaving the College depending on circumstances.
- 13.3 In general all information will be kept for 4 years after a member of staff leaves the College. Some information however will be kept for much longer. This will include information necessary in respect of pensions, taxation, potential or current disputes or litigation regarding employment and information required for job references. A full list of information with retention times is available from the Head of HR.
- 13.4 The College will safely destroy data, (e.g. using shredders on College premises) when it is no longer required and in line with the periods indicated above (see 13.1). For large quantities of documents containing personal and other data, the College shall only use recognised companies for this purpose. The College will employ similar approaches to the destruction of electronic data. When this is held on computer drives the College shall employ registered companies for this purpose specifically in relation to drives in PCs.
- 13.5 Data captured digitally via CCTV will normally be kept for 31 days and destroyed thereafter. The exception to this is when this data is required to support crime detection and subsequent legal proceedings

**14. Conclusion**

- 14.1 Compliance with the 1998 Act is the responsibility of the College. Any deliberate breach of this Data Protection Policy may lead to disciplinary action being taken, or access to College facilities being withdrawn, or even criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should take it up with a designated data controller.
- 14.2 This policy will be reviewed every 2 years unless further legislation necessitates an earlier review date.

## **Appendix 1**

### **Staff Guidelines for Data Protection**

1. The College collects data from learners to allow staff to process data about learners on a regular basis and enable them to perform their duties. For example when marking registers or College work, writing reports or references, or as part of a pastoral or academic supervisory role. The College will ensure through registration procedures that all learners give their consent to this sort of processing and are notified of the categories of processing as required by the 1998 Act.
2. The information that staff deal with on a day-to-day basis will be standard and will cover categories such as: general personal details such as name and address, details about class attendance, course work marks and grades and associated comments and notes on personal supervision, including matters about behaviour and discipline.

### ***Sensitive (or Restricted Data)***

3. Information about a learner's physical and mental health; sexual life; political or religious views; trade union membership; ethnicity or race is sensitive and can only be collected and processed with the learner's consent. If staff need to record this information, they should use the College standard form e.g. recording information about dietary needs, for religious or health reasons prior to taking learners on field trips; recording information that a learner is pregnant, as part of pastoral duties.
4. Staff have a duty to make sure that they comply with the data protection principles, which are set out in the College's Data Protection Policy which is available on the College's Website and Intranet. In particular staff must ensure that records are accurate, up to date and disposed of safely and in accordance with College policy.
5. The College will designate staff in each area as "authorised staff". Data controllers in functional areas will perform this function in respect of standard data. Course Tutors and their direct line manager will perform this in their academic area. These staff are the only staff authorised to hold or process data that is not standard data; e.g. sensitive data.
6. The only exception to this will be if a non-authorised staff member is satisfied that the processing of this data is necessary, in the best interest (e.g. for reasons of welfare, health and health and safety) of the learner or staff member, or a third person, or the College; he or she has either informed the authorised person of this or has been unable to do so and processing is urgent and necessary.
7. This should only happen in very limited circumstances e.g. if a learner is injured or unconscious and in need of medical attention, and when a staff tutor needs to inform any medical person or authority of any health circumstances or religious reasons which may inform the nature of medical attention the learner may receive.
8. Authorised staff will be responsible for ensuring that all data is kept securely.

9. Staff must not disclose personal data to any learner, unless for normal academic or pastoral purposes without authorisation or agreement from the data controller, or in line with the College policy.
10. Staff shall not disclose personal data to any other staff member except with the authorisation or agreement from the data controller, or in line with the College policy.
11. Staff shall inform their line manager and / or the Principal of any suspected breach in data security (see appendix 2)

***Checklist***

12. Before processing any personal data, all staff should consider the check list:-
  - a) Do you really need to record the information?
  - b) Is the information “standard” or is it “sensitive”?
  - c) If it is “sensitive” do you have the data subject’s express consent?
  - d) Has the learner been informed how and that this type of data will be processed?
  - e) Are you authorised to collect/store/process the data?
  - f) If yes, have you checked with the data subject that the data is accurate?
  - g) Are you sure the data is secure?
  - h) If you do not have the data subject's consent to process, are you satisfied that it is in the best interests of the learner or the staff member to collect and retain the data?
  - i) Have you reported the fact of data collection to the authorised person within the required time?
  - j) Have you inadvertently copied personal data on a personal portable computer or portable disk drive? Or if other documents are held on such devices is the data encrypted?
  - k) If you work in a function (e.g. Learner services, Information services or Campus Service Office) where most of the data is collected have you brought to the attention of the learner the consent to capture data on the enrolment form?
  - l) Do you have secure lockers or other facility to safely store personal data in your area of work? If not have you informed your line manager?

## Appendix 2

### Data Security - Breach Management Plan

- a) The DP Policy cites that a suspected or actual data security breach should be notified to the Principal / Chief Executive. This notification should provide an early assessment of the cause, e.g.
  - Loss or theft of data or equipment on which data is stored
  - Inappropriate access controls allowing unauthorised use
  - Equipment failure
  - Human error
  - Unforeseen circumstances such as a fire or flood
  - Hacking attack
  - ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.
- b) The Principal / Chief Executive (or Deputy Principal) shall then appoint a designated manager to investigate the breach. The investigating officer should be one of the Data Controllers and may involve input from specialists across the College such as IT, HR, Learner Services and in some cases also include external stakeholders.
- c) The investigation will normally be concluded in 10 working and the report, with recommendations, should include the following elements:-
  - Containment and recovery
  - Assessment of ongoing risk
  - Notification of breach – if necessary
  - Evaluation and response to what will be done to avoid a similar event in the future

The attached Annexes: ‘*Guidance on data security breach management*’ should be used as guidance by the investigating officer in executing the investigation and the completion of the report.

This initial phase (a-c) however should determine at the earliest opportunity if the breach is serious enough to warrant the breach having to be notified to the ICO.

- d) The investigation and production of complete report with recommendations is required to be completed usually within 14 working days, albeit this may need to be extended depending on circumstance, albeit this potential extension should not restrict reporting on progress.
- e) The outcome of the evaluation and response should be included as an update to the existing Data Protection Policy within 30 days of the completion of the investigation, albeit a notice could be posted on the intranet prior to this timescale.

**Appendix 2a: Guidance notes on factors to be considered in the event of a data security breach (to assist in deciding an appropriate course of action):**

a) Reasons for a data security breach

- Loss or theft of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Equipment failure
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking attack
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it.

The four important elements of the breach management plan:

- Containment and recovery
- Assessment of ongoing risk
- Notification of breach
- Evaluation and response

**1. Containment and recovery**

Involvement in this element may require input from specialists across the College such as IT, HR and Learner Services legal (and in some cases contact with external stakeholders).

Factors to be considered: -

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise. This could be isolating or closing a compromised section of the network, finding a lost piece of equipment or simply changing the access codes at the front door.
- Establish whether there is anything you can do to recover any losses and limit the damage the breach can cause. As well as the physical recovery of equipment, this could involve the use of backup tapes to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts
- Where appropriate, inform the police

**2. Assessing the risks**

Some data security breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. An example might be where a laptop is irreparably damaged but its files were backed up and can be recovered, albeit at some cost to the business.

While these types of incidents can still have significant consequences the risks are very different from those posed by, for example, the theft of a customer database, the data on which may be used to commit identity fraud.

Before deciding on what steps are necessary further to immediate containment, assess the risks which may be associated with the breach. Perhaps most important is an assessment of potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen. Points to be considered in risk assessment: -

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health – criminal records) while other data types are sensitive because of what might happen if it is misused (bank account details)
- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data? 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
- Regardless of what has happened to the data, what could the data tell a third party about the individual? 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
- How many individuals' personal data are affected by the breach? It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment
- Who are the individuals whose data has been breached? Whether they are staff, customers, clients or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, your actions in attempting to mitigate those risks
- What harm can come to those individuals? Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- 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.

### **3. Notification of breaches**

Informing people and organisations that you have experienced a data security breach can be an important element in your breach management strategy. However, informing people about a breach is not an end in itself. Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints. Answering the following questions will assist you in deciding whether to notify:

- Are there any legal or contractual requirements? At present, there is no law expressly requiring you to notify a breach but sector specific rules may lead you towards issuing a notification
- Can notification help you meet your security obligations with regard to the seventh data protection principle?
- Can notification help the individual? Bearing in mind the potential effects of the breach, could individuals act on the information you provide to mitigate risks, for example by cancelling a credit card or changing a password?
- If a large number of people are affected, or there are very serious consequences,
- Consider how notification can be made appropriate for particular groups of individuals, for example, if you are notifying children or vulnerable adults.

- Have you considered the dangers of ‘over notifying’. Not every incident will warrant notification and notifying a whole 20,000 strong customer base of an issue affecting only 2,000 customers may well cause disproportionate enquiries and work.
- You also need to consider who to notify, what you are going to tell them and how you are going to communicate the message. This will depend to a large extent on the nature of the breach but the following points may be relevant to your decision:
- Make sure you notify the appropriate regulatory body. A sector specific regulator may require you to notify them of any type of breach but the ICO should only be notified when the breach involves personal data
- 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
- Your notification should at the very least include a description of how and when the breach occurred and what data was involved. Include details of what you have already 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 you are willing to do to help them
- Provide a way in which they can contact you for further information or to ask you questions about what has occurred – this could be a helpline number or a web page, for example.

When notifying the ICO you should also include details of the security measures in place such as encryption and, where appropriate, details of the security procedures you had in place at the time the breach occurred. You should also inform us if the media are aware of the breach so that we can manage any increase in enquiries from the public. When informing the media, it is useful to inform them whether you have contacted the ICO and what action is being taken. The ICO will not normally tell the media or other their parties about a breach notified to us, but we may advise you to do so. Refer to ICO Guidance on Breach Notification in the next section, or visit

[http://www.ico.gov.uk/Home/what\\_we\\_cover/data\\_protection/guidance/good\\_practice\\_notes.asp](http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/good_practice_notes.asp)  
[x](#)

You might also need to consider notifying third parties such as the police, insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss to individuals, and trade unions.

#### **4. Evaluation and response**

It is important not only to investigate the causes of the breach but also to evaluate the effectiveness of your response to it. Clearly, if the breach was caused, even in part, by systemic and ongoing problems, then simply containing the breach and continuing ‘business as usual’ is not acceptable; similarly, if your response was hampered by inadequate policies or a lack of a clear allocation of responsibility then it is important to review and update these policies and lines responsibility in the light of experience. You may find that existing procedures could lead to another breach and you will need to identify where improvements can be made.

The following points will assist:

- Make sure what personal data is held and where and how it is stored. Dealing with a data security breach is much easier if you know which data are involved. Your notification with the Information Commissioner will be a useful starting point.
- Establish where the biggest risks lie. For example, how much sensitive personal data do you hold? Do you store data across the business or is it concentrated in one location?

- Risks will arise when sharing with or disclosing to others. You should make sure not only that the method of transmission is secure but also that you only share or disclose the minimum amount of data necessary. By doing this, even if a breach occurs, the risks are reduced
- Identify weak points in your existing security measures such as the use of portable storage devices or access to public networks
- Monitor staff awareness of security issues and look to fill any gaps through training or tailored advice
- Consider whether you need to establish a group of technical and nontechnical staff who discuss ‘what if’ scenarios – this would highlight risks and weaknesses as well as giving staff at different levels the opportunity to suggest solutions
- If your organisation already has a Business Continuity Plan for dealing with serious incidents, consider implementing a similar plan for data security breaches
- It is recommended that at the very least you identify a group of people responsible for reacting to reported breaches of security

## **Appendix 2b: Guidance Notes regarding Notification of any Data Security Breaches to the Information Commissioner's Office**

- All data controllers have a responsibility under the Data Protection Act 1998 to ensure appropriate and proportionate security of the personal data they hold. (DPA 1998 7th Principle).
- Although there is no legal obligation on data controllers to report breaches of security which result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to the attention of his Office.
- The nature of the breach or loss can then be considered together with whether the data controller is properly meeting his responsibilities under the DPA. "Serious breaches" are not defined.

### **Factors determining whether breaches should be reported and potential consequences of reporting a 'breach'**

#### **a) The potential harm to data subjects:**

The potential harm to individuals is the overriding consideration in deciding whether a breach of data security should be reported to the Information Commissioner's Office.

Ways in which harm can occur include:

- o exposure to identity theft through the release of non-public identifiers eg passport number
- o information about the private aspects of a person's life becoming known to others eg financial circumstances.

The extent of harm, which can include distress, is dependent on both the volume of personal data involved and the sensitivity of the data. Where there is significant actual or potential harm as a result of the breach, whether because of the volume of data, its sensitivity or a combination of the two, there should be a presumption to report. Where there is little risk that individual would suffer significant harm, for example because a stolen laptop is properly encrypted, or the information that is the subject of the breach is publicly available information, there is no need to report.

#### **b) The volume of personal data lost / released / corrupted:**

- 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. It is difficult to be precise what constitutes a large volume of personal data. Every case must be considered on its own merits but a reasonable rule of thumb is any collection containing information about 1000 or more individuals.
- An example we would expect to be reported would be the theft / loss of an *unencrypted* laptop computer or other *unencrypted* portable electronic / digital media holding names and addresses, dates of birth and National Insurance Numbers of 1000 individuals.
- An example we would not expect to be reported would be the theft / loss of a marketing list of 500 names and addresses or other contact details where there is no particular sensitivity of the product being marketed.

- However it may be appropriate to report much lower volumes in some circumstances where the risk is particularly high perhaps because of the circumstances of the loss or the extent of information about each individual. If the data controller is unsure whether to report or not, then the presumption should be to report.

**c) The sensitivity of the data lost / released / unlawfully corrupted:**

- There should be a presumption to report to the ICO where smaller amounts of personal data are involved, the release of which could cause a significant risk of individuals suffering substantial harm. This is most likely to be the case where that data is sensitive personal data as defined in section 2 of the DPA.
- As few as 10 records could be the trigger if the information is particularly sensitive. An example we would expect to be reported would be a manual paper based filing system (or unencrypted digital media) holding the personal data relating to 50 named individuals and their financial records. An example we would not expect to be reported would be a similar system holding the trade union subscription records of the same number of individuals where there were no special circumstances surrounding the loss.

**d) Reporting**

Serious breaches should be notified to the Information Commissioner's Office by email using the address [casework@ico.gsi.gov.uk](mailto:casework@ico.gsi.gov.uk), or by post to our office address: *Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF*. The notification should include:

- o The type of information and number of records
- o The circumstances of the loss / release / corruption
- o Action taken to minimise / mitigate effect on individuals involved including whether they have been informed
- o Details of how the breach is being investigated
- o Whether any other regulatory body has been informed and their response
- o Remedial action taken to prevent future occurrence
- o Any other information you feel may assist us in making an assessment

Guidance on how to manage a data security breach can be found here:

[http://www.ico.gov.uk/Home/what\\_we\\_cover/data\\_protection/guidance/good\\_practice\\_notes.aspx](http://www.ico.gov.uk/Home/what_we_cover/data_protection/guidance/good_practice_notes.aspx)

**e) What will the Information Commissioner's Office do when a breach is reported?**

The nature and seriousness of the breach and the adequacy of any remedial action will be assessed and a course of action determined. We may:

- o Record the breach and take no further action
- o Investigate the circumstances of the breach and any remedial action which could lead to:
  - 1) no further action
  - 2) a requirement on the data controller to undertake a course of action to prevent further breaches

- 3) formal enforcement action turning such a requirement into a legal obligation 4)  
Where there is evidence of a serious, deliberate or reckless breach of the DPA, the serving of a monetary penalty notice requiring the organisation to pay a monetary penalty of an amount determined by the Commissioner up to the value of **£500,000**

Where a breach has been voluntarily reported to the ICO, we will take this into consideration when deciding on the most appropriate course of action.

**f) Will a reported breach be made public?**

- We do not see it as our responsibility to publicise security breaches not already in the public domain or to inform any individuals affected. In so far as they arise these are the responsibilities of the data controller.
- However, the ICO may recommend the data controller to make a breach public where it is clearly in the interests of the individuals concerned or there is a strong public interest argument to do so.
- Where the Information Commissioner takes regulatory action, it is policy to publicise such action, unless there are exceptional reasons not to do so. This policy on publication extends to any formal undertakings provided to the Commissioner by a data controller.
- However the Commissioner will not normally take regulatory action unless a data controller declines to take any recommended action, he has other reasons to doubt future compliance or there is a need to provide reassurance to the public. Such a need is most likely to arise where the circumstances of the breach are already in the public domain.
- Further information on the ICO's regulatory action strategy can be found here: [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/data\\_protection\\_regulatory\\_action\\_policy.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/data_protection_regulatory_action_policy.pdf)

More information on monetary penalties can be found here:

[http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/ico\\_guidance\\_monetary\\_penalties.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf)

### **Appendix 3: Role of Data Controllers**

The College has a number of designated data controllers. These include:

- Head of HR,
- Head of Learner Services,
- Assistant Estates Manager,
- Data Management Manager
- Campus Service Office Managers
- Head of Finance and
- Curriculum Director representative

The College also has a number of authorised staff (Line Managers) in academic areas to manage and deal with data, including sensitive data relating to learners.

#### **Key Roles – Tasks**

- Ensure Processes are well developed and documented in dealing with personal and sensitive data, ensuring at all times that staff within functional and academic areas comply with laid down procedures (in compliance with this policy)
- Contribute when necessary to any investigation relating to a suspected or actual breach in data security.
- Undertake when necessary staff updates, awareness-raising and development sessions (with support from HR) within their area of responsibility
- Ensure that they authorise and control proper destruction of data in line with this policy where data records may be required to be kept beyond a 7 year period. Cognisance should also be taken of the Document Retention Policy (*currently in draft & awaiting approval by governors*).