

Business and Community Engagement



Data Protection and BCE

This publication is aimed at UK further and higher education staff working in areas related to knowledge transfer, work based learning, community links, outreach, CPD, employer engagement, wider, and lifelong learning.

It is one of a series of publications produced by JISC Legal to raise awareness of the potential legal issues related to the use of technology by colleges and universities in relation to their business and community engagement activities.

Please note: this guidance has been prepared by **JISC Legal** for information purposes only and is not, nor is intended to be, legal advice. This information is not intended to constitute, and receipt of it does not constitute, a contract for legal advice or the establishment of a solicitor-client relationship.

20 June 2007

If you have Adobe Acrobat Reader installed on your computer, you may download a PDF version here - <http://www.jisclegal.ac.uk/pdfs/BCEdataprotect.pdf>.
(Recommended for printing.) Acrobat Reader is available free from Adobe's web site - <http://www.adobe.com/>.

Table of Contents

1. Introduction	1
2. Acting in What Capacity?.....	2
3. What Data and What Purposes?	3
4. Fair Processing Notice	3
5. Grounds for Processing	3
6. Notification	4
7. Research.....	4
8. Subject Access.....	5
9. Transfers Outside the EEA	6
10. Marketing	6
11. Conclusion.....	7

1. Introduction

Colleges and universities have to consider all aspects of their operations when seeking to ensure compliance with the Data Protection Act 1998 ("the Act"). These operations cover the institution's core teaching and administration functions, its research activity, but also extend to BCE activities.

BCE activities will often involve the collection and use of personal data. Accordingly, institutions must ensure that their policies, practices and procedures cover any processing which they undertake in the course of these activities.

This briefing note considers the data protection law implications which may arise when an institution is involved in Business and Community Engagement (“BCE”) activities.

For more general information about data protection for UK further and higher education institutions, JISC Legal’s guidance is available at - <http://www.jisclegal.ac.uk/dataprotection/DataProtectionPub.htm>.

2. Acting in What Capacity?

The institution has to establish the capacity in which it is acting (in data protection terms) when carrying out the BCE activity. Is it a data controller or a data processor?

Examples

- (1) The institution runs a training course for members of a particular industry. Any organisation within that industry can send its employees to the course. In this case, the institution will generally be the **data controller**. It will determine the purposes for which the data is collected and processed, namely, the administration of the course and connected purposes. Basically, it has control of the data. It may make some of this data available to the respective organisations – for example, attendance records and assessment results – in which case those organisations will also become data controllers in respect of the data provided to them.
- (2) Bloggs Limited used to conduct all of its training in-house through its own training unit. This unit, however, was recently disbanded and now training is outsourced to a college. The company’s contract with the college specifies what the training is to cover, the key areas of assessment, where the data is to be stored and how it is to be reported by the institution. It also states that the institution may only use the data which it collects or generates for the purposes specified by the company. In this respect, the institution will be acting as a **data processor**. It has no say over how that data is used – rather, it is simply processing the data on the company’s behalf. In some cases, the outsourcing contract itself may confirm that the service provider is acting as a data processor.

In the examples above, the key difference lies in the institution’s role. When it runs the training course for the industry members, it is doing so on its own account. It determines the manner in which the data is collected and the purposes for which it is used. In the other scenario, the institution is just performing the processing function for Bloggs Limited.

This distinction is important because, where an institution is acting as data controller, the institution will have to comply with the requirements and obligations imposed by the Act. These obligations do not apply to data processors – the controller, however, must impose some obligations on the processor by way of contract.

As a minimum, the processor should be obliged to act only on the data controller's instructions when processing the data and take appropriate technical and organisational measures to protect it. In some cases the obligations imposed may be far wider than this. For instance, the customer may require that the institution complies with the principles set out in the Act as if it were the data controller and that the institution does nothing which places the data controller in breach of its obligations under the Act.

This means that if the institution fails to comply with the data processing principles, the customer (as data controller) will be in breach of the Act. The customer will then have a contractual remedy against the institution for failing to comply with its obligations under the contract.

Accordingly, where personal data is involved, the institution must establish the capacity in which it will be acting in that project. If it acts as data controller, it will be subject to the obligations set out in the Act. If it is simply carrying out a processing function, the institution should establish the extent to which those obligations are imposed on it by way of contract.

Whilst the examples above concern training, the same principles apply to other activities, such as, for instance, research conducted by an institution.

3. What Data and What Purposes?

When carrying out a BCE activity, the institution should establish what personal data it will collect and/or generate, and the purposes for which that data will be used. This will enable the institution to prepare its fair processing notice and consider the grounds on which the processing will take place.

4. Fair Processing Notice

The fair processing notice should identify the data controller and what the data will be used for. This information should generally be provided when the data is collected and any non-obvious processing purposes should be stated.

Fair Processing

In example (1) above, the fair processing information may be provided to the individual when he or she signs up for the course (for instance, on the application form). If the employer completes the form on the individual's behalf, the information could be sent to the employee, perhaps as part of a welcome letter.

If there is any doubt about whether a processing purpose is (or is not) obvious, then it may be best to err on the side of caution. So, for instance, if details of the individual's performance or attendance are to be reported back to the employer, the institution may wish to advise the individual of this.

5. Grounds for Processing

The Act requires that a data controller has grounds for its processing. There are a number of general grounds which apply to all personal data (Schedule 2 Conditions), and additional grounds which apply where sensitive personal data is involved (Schedule 3 Conditions). It is imperative that the data controller can justify its

processing on the basis of these grounds. An assessment of the data will therefore allow the institution to assess what grounds (if any) apply and whether consent should be obtained.

Grounds

Following on from the first example above, the institution maintains a computerised record of course attendance and absences. It justifies processing this data on the basis that the individual has consented. The fair processing information was set out on the registration form completed by the applicant and it was made clear that non-attendance would be reported to the employer.

On one occasion, John Smith didn't turn up for the course. The following week, he told the course leader that he missed the class because he had been in police custody. He had been questioned about an alleged assault and had been charged.

At the end of that month, the institution sent details of John Smith's attendance to his employer together with the reason why he missed that particular day. John Smith is now rather annoyed that his employers have found out about his alleged misdemeanour, but the institution claims that it had his consent to provide attendance details.

Leaving aside the other Schedule 2 conditions, the institution could well justify disclosure of the failure to attend on the basis of consent. He was advised that this would take place and signed up to the course with this knowledge.

This justification, however, would not extend to disclosure of the reason for non-attendance. This information was sensitive personal data and so disclosure could only be made with the individual's explicit consent, or on the basis of another Schedule 3 condition.

Whilst the example above concerns details about an alleged offence, the same principles would apply, for instance, to non-attendance for physical or mental health issues, trade union membership or religion. Ideally, the institution should have disclosed only the failure to attend. The employer could then have sought an explanation from the employee. Alternatively, if reasons for non-attendance were to be provided, the scope of this should have been made clear to the data subject and his or her explicit consent obtained. It demonstrates, however, that there can be a thin line between legitimate and unlawful disclosures.

6. Notification

The institution must consider whether its notification is complete and reflects the full range of its activities. Whilst an institution may have notified the processing which it carries out in the context of its teaching, administration, support and research functions, if it does take part in BCE activities, the notification should reflect this. So, for instance, some institutions should specify that they provide commercial services, such as consultancy services or facilities hire. It is important to remember that failure to be properly notified is a criminal offence.

7. Research

An institution may provide research services to various parties – this could include the business community, central or local government departments, charities and community organisations. These services will often involve the processing of

personal data and this processing is caught by the Act. There are however certain exemptions for "research purposes." For instance, if the processing is not used to support measures or decisions targeted at particular individuals and it does not cause substantial distress or damage to a data subject, the personal data:-

- can be processed for purposes other than those for which they were originally obtained;
- can be held indefinitely; and
- is exempt from the data subject's right of access

where the data is processed for research purposes and the results do not identify data subjects.

Also, it is expressly permitted to process sensitive personal data for research purposes 'in the substantial public interest' without explicit consent where the sensitive personal data is not used to support measures or decisions targeted at particular individuals and no substantial damage or distress is caused, or is likely to be caused, to any person by the keeping of those data.

It is important to remember that while some exemptions are granted for the use of personal data for research purposes, there is no blanket exemption from all the Data Protection Principles. Personal data obtained or otherwise processed through research activity should be obtained and processed fairly and lawfully. Data subjects should be made aware of what their data will be used for and should still be informed of any new purposes of data processing. They should also be advised of the identity of the data controller and any disclosures that may be made. Consideration may also be given to anonymising the data, as anonymous data are not covered by the Act.

8. Subject Access

Most institutions will be familiar with subject access requests being submitted by current or former staff or students. Where the institution undertakes BCE activities, it could well receive subject access requests from those individuals to whom the services in question were provided (i.e. course attendees).

This means that the institution's procedures (and the person(s) responsible for dealing with subject access requests) must recognise this potential new category of data subject. Even though the person is not a student or staff member, s/he can still be a data subject for the institution's purposes. The key issue is whether or not the institution processes that person's personal data. It also reinforces the need for the institution to be sure of the capacity in which it is acting when providing BCE activities. If it is not a data controller, it should not respond to the subject access request and should instead refer the individual to the data controller.

9. Transfers Outside the EEA

The Act limits the transfer of personal data to countries within the EEA – this covers the EU member states plus Iceland, Liechtenstein and Norway.

Example

(3) The institution has received a request from a company in the United States. This company has a Glasgow-based subsidiary and wishes to enrol a number of its employees on a health and safety course. It has requested that attendance details and assessment results are forwarded directly to its main personnel team in the US, as all training issues are dealt with centrally at head office. Can the institution do this?

In the example above, the institution could only transfer the personal data outside the EEA where the recipient country (i.e. the US) offers adequate protection to that provided by the Act. Failing this, the institution would have to try and bring itself within one of the derogations.

The European Commission recognises several countries as having adequate protection (such as Argentina, Switzerland and the Isle of Man). Transfers to the US are also permitted where the recipient company has signed up to the US “Safe Harbor” regime. It is important to note that Safe Harbor is company specific and not countrywide. Accordingly, the data controller must check the US Department of Commerce’s Safe Harbor list to make sure that the recipient company is listed.

Adequate protection may also be supplied by the adoption of contractual obligations to treat the data to standards equivalent to those imposed by the Act. The European Commission has issued two model form contracts and if the data is exported as part of a contract which incorporates the model clauses the protection provided by the contract is deemed to be adequate.

If none of these options applies the controller must either bring itself within one of the derogations or make its own assessment of adequacy of protection. The derogations include the ground that the data subject has given consent to the transfer and many data controllers seek consent to overseas transfers as a matter of routine under contracts with data subjects.

The transfer of personal data overseas is a difficult area. There are doubts about the effectiveness of Safe Harbor and the European Commission’s model contracts are not without their difficulties. Institutions should review their arrangements in this area and may need to take specific advice. In this example, perhaps the best and most efficient course of action would be for the institution to seek the consent of the data subjects to the proposed transfers. If the employer forces its employees to consent, however, this could undermine the validity of that consent.

10. Marketing

An institution (or indeed any business) can provide the best service or product in the world, but if no one knows about it, that product or service will not be very

successful. BCE activity will inevitably involve an element of marketing to let other organisations know what the institution can offer them. Marketing by phone, fax or email however has to be conducted in accordance with the Privacy and Electronic Communications (EC Directive) Regulations 2003 (“the Marketing Regulations”).

By Phone or Fax

Unsolicited marketing calls should not be made to individual subscribers who have opted-out either directly or by registering with the central stop-list, the Telephone Preference Service (TPS). Nor should they be made to corporate subscribers (e.g. companies) who have objected either directly or by registering on the Corporate TPS.

Unsolicited marketing faxes should not be sent to individuals without their prior consent or to any subscriber who has objected, either directly or by registering on the Fax Preference Service (FPS).

By Email

Unsolicited marketing emails or SMS should only be sent to an individual subscriber who has consented unless the email address or phone number was collected in the context of a commercial relationship (i.e. a previous project or provision of a service). The marketing emails must involve similar goods or services and an opt-out must be provided with each marketing email.

11. Conclusion

Most institutions will already have data protection policies and procedures in place. In terms of BCE activity, the issue is to ensure that those policies and procedures (and the individuals within the institution) recognise and cater for those extended activities. Institutions should not reinvent the wheel. They can certainly use their existing policies, procedures and experience as the relevant data protection rules and underlying principles are the same regardless of the activity. The difference lies in the change of context, the differing roles of the parties and the considerations which arise from that.

Summary

In summary, for its BCE activities, the college or university should:-

- know the capacity in which it is acting (i.e. controller or processor);
- know what data it is processing and the purposes for which it is being processed;
- ensure that the data is collected fairly;
- be able to justify its grounds for processing that data;
- ensure that its notification covers the activity in question;
- recognise third parties (other than staff or students) as potential data subjects;
- ensure that it only transfers personal data outside the EEA where appropriate safeguards are in place;
- ensure that its marketing practices comply with the Marketing Regulations.

20 June 2007