University of Brighton

Data Protection Policy

Contents

Paragraph

1 Introduction

The University of Brighton needs to keep certain information about its employees, students and other users to allow it to monitor such areas as performance, achievements, and health and safety. It is also necessary to process the information so that staff can be recruited and paid, courses organised and legal obligations to funding bodies and government met.

This policy has been written to ensure that the University of Brighton complies with legal requirements in the handling of personal information. The Data Protection Act 1998 (DPA) specifies eight principles (see Appendix 1) which must be observed by all staff, students, or others dealing with personal data* on behalf of the University. Both computer and manual records, including filing systems and holdings on fiche, are covered.

Terms marked with an asterisk are defined in Appendix 2.

2 Status of the policy

2.1 Staff

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 University of Brighton. Any breach of this data protection policy will be treated as a serious matter.

2.2 Students

This policy does not form part of the formal contract between the University of Brighton and the student but, as stated in the Student Handbook, students must observe and abide by the University's policies. Any breach of this data protection policy will be treated as a serious matter.

3 The Data Controller*

The University of Brighton as a body corporate is the data controller under the DPA, and the Board of Governors is therefore ultimately responsible for implementation. However, the Legal Adviser is the university's Designated Data Protection Officer and is responsible for dealing with day to day matters.

In matters of collaboration and partnership with other bodies, it is possible for either or both organisations to be the data controller, depending upon the nature of the agreement or contract. Please refer any queries to the Legal Adviser.

4 Notification of data* held and processed*

The University of Brighton undertakes to maintain an accurate and timely notification of its data processing activities with the Information Commissioner's Office (ICO). The university is registered as a Data Controller and its registration number with the ICO is **Z5395727**

5 Staff and student data

All staff, students and other users are entitled to know:

- what information the University of Brighton holds and processes about them and why (see Appendix 3)
- how to gain access to it
- how to keep it up-to-date
- what the University of Brighton is doing to comply with its obligations under the DPA

Anyone who considers that the policy has not been followed in respect of personal data about him/herself should discuss the matter with his/her head of school/department in the first instance. If the matter is not resolved it should be raised with the Legal Adviser.

6 Publication of information by the University of Brighton

The University of Brighton is committed to openness and accessibility in the provision of information for all aspects of its work, having due regard to issues of efficiency, legality, security and confidentiality. Information that is already in the public domain is exempt from the DPA and it is university policy that certain types of information will normally be available via the university website, including but not limited to the following:

- names of members of staff with university contact details
- names and images of the University Board of Governors
- names and images of the Senior Management Team

The University of Brighton internal phone list will not be a public document but it will be possible to find details of telephone extension, email address and department for any member of staff by a name search through the website. Any individual who has good reason for wishing details in these lists or categories to remain confidential should contact his/her Head of School or Department in the first instance. If this fails to resolve the matter, then it should be raised with the Legal Adviser.

Images, either of individuals or small groups, will not normally be displayed on the University website or used in other promotional material without the explicit consent of the individuals involved. However, images of large groups at public events, where it would not be practicable to approach each person individually, may be used freely. Further information and clarification may be obtained from the Legal Adviser.

Please see Appendix 6 for further details of the University's policy concerning publication of staff photographs

6.3 UniCard

Personal information held on the UniCard Database will be treated confidentially and under the terms of the Data Protection Act 1998 will only be used for the purposes of card administration, and where necessary, extracted and shared with other departments to enable members of staff, students and associates to access University facilities and services.

The University may share information held on UniCard with other departments of the University and / or appointed agents: to provide users with the service applied for; to help resolve a complaint, for analysis and / or Management Information; or: for purposes of fraud prevention, audit or debt collection; other cardholders, but only where it is considered necessary for resolution of fraud or dispute and for the investigation of crime or in connection with disciplinary investigations.

As a User, you are entitled to make a Subject Access Request for a copy of any personal data about you held on computer. Users wishing to make such a request should write to the University's Information Policy Officer for a copy of the application form. The fee for each subject access request is £10.00. This fee is set by the Information Commissioner, not by the University.

Data will be processed in accordance with relevant legislation and, specifically, in accordance with the provisions of the Regulation of Investigatory Powers Act (2000).Unless specifically requested, for legislative or academic reasons, personal UniCard data will be archived from the system 90 days after card expiry date or when the user of the UniCard is no longer employed by the university or is not attending any course.

Access Control Records

Access control records will be processed in strict accordance with the Data Protection Act. Records relating to an individual's use of the Unicard to gain access to University premises will not routinely be divulged to any third parties. This information may lawfully be disclosed, however, in connection with a disciplinary or criminal investigation or because of health and safety concerns. Such disclosure is subject to the specific authorisation of a member of the University's Senior Management team.

Access control data will normally be retained on the system for 90 days only, and will then be archived. After 180 days the records will be deleted. All access control records are deleted 90 days after the card holder ceases to be a student or member of staff of the University.

Please see UniCard Webpages (https://unicard.brighton.ac.uk/cms/) for further details of the terms and conditions for UniCard.

7 Responsibilities of staff

7.1 Personal information

All staff are responsible for:

- checking that any information that they provide to the University of Brighton in connection with their employment is accurate and up-to-date
- informing the University of Brighton of any changes to information already provided, e.g. new address
- checking any information that the University of Brighton sends to them to verify contact and other personal information
- notifying the University of Brighton of any errors or necessary amendments. The University of Brighton cannot be held responsible for any inaccuracies unless the staff member has previously provided the University with the correct information

7.2 Security of Personal Data

All staff are responsible for ensuring that:

- they are familiar with and observe the Staff Guidelines for the Handling of Personal Data (see Appendix 4)
- any personal data which they hold is kept securely
- personal data is not disclosed either orally or in writing, accidentally or otherwise, to any unauthorised third party
- any personal data held on a computer is secured

- staff should note that Personal Data must never be stored on portable data storage devices (such as USB sticks or hard drives unless encrypted.

Staff should note that unauthorised disclosure will be considered a serious matter.

7.3 Data security: dealing with third party enquiries

The University of Brighton is committed to data security, and will make every effort to safeguard against illegitimate disclosure of personal information. Where a request for personal information is received from a third party, the identity of that third party and the need for the information must be established before disclosure is even considered (see Appendix 5 Guidelines for the disclosure of student personal data). Enquiries/requests for disclosure from the Police should be directed to the Legal Adviser.

In all cases, if there is any doubt as to the validity of the enquirer or their enquiry, no disclosure should be made and the caller should be directed to the Legal Adviser.

8 Student Responsibilities

8.1 Personal information

All students are responsible for:

- checking that information they provide to the University of Brighton in connection with their membership of the university is accurate and up-to-date

- advising the University of Brighton of any amendments to this information, e.g. changes of address. The University of Brighton cannot be held responsible for any errors unless the student has provided updated information as here requested.

8.2 Students who process personal data

Students who need to process personal data as a justifiable part of their studies (whatever the level or mode) will be covered by the University of Brighton's Data Protection notification. They will be expected to observe the relevant guidelines issued by the university. Should they be processing on behalf of another organisation, whilst on placement for example, they will be bound by the Data Protection policies and provisions of that body as the Data Controller.

9 Research and consultancy

Staff and, where relevant, students engaging in research will be covered by the University of Brighton's Data Protection notification. Provided that any research undertaken is not published in a way that would identify individuals or cause them damage or distress, data used for research purposes has certain exemptions from the terms of the Act. In practice, this means:

- there is no right of subject access to personal data where the information has been anonymised for research purposes and where the results do not identify individuals (see 11 Rights to access information)
- personal data may be held indefinitely

Despite the terms of these exemptions, the University of Brighton seeks to ensure that, wherever practically possible, data subjects are made fully aware of any research for which their personal data may be used. Researchers are required to keep their data secure and to guard against any accidental disclosure that might arise from direct or indirect reference to individuals in any research report.

Consultancy undertaken for and on behalf of an organisation other than the University of Brighton may be subject to the Data Protection policy and provisions of that organisation as well as those of the university, depending upon the nature of the agreement or contract. Please refer any queries to the Legal Adviser.

10 CCTV

The University operates a CCTV monitoring system around its properties. The function of this system is to assist in the detection and deterrence of crime and to assist the Police and civil authorities in the event of a major emergency. The system will be operated in such as way as to safeguard individuals' right to privacy.

All CCTV images have ownership and copyright vested in the University of Brighton. Cameras will be mounted in public view and signs will be displayed warning of their presence and the purposes of their operation. Recorded images will normally be preserved for a period to be determined in accordance with the University Records Retention Schedules. After this period, if they are not needed for evidential purposes, the recording media will be re-used. If required for evidential purposes, they will be retained for as long as is necessary to the prosecution of the case. Requests for access to images should be channelled through the Legal Adviser.

11 Rights to access information

11.1 Subject Access request

Staff, students and other users of the University of Brighton have the right to access any personal data that is being kept about them either on computer or in manual files. Whilst such a request (known as a "Subject Access Request") can be made in any format, individuals wishing to exercise this right may wish to complete the University of Brighton Subject Access Form in order to provide sufficient information to identify the documents requested:

(http://staffcentral.brighton.ac.uk/xpedio/groups/public/documents/staffcentral/doc001915.pdf)

and send it to the Legal Adviser.

The University of Brighton will normally make a charge of £10 on each occasion that access is requested by persons no longer employed or no longer studying at the institution. The university reserves the right to make the same charge to current staff and students. Suitable proof of identity may be required.

The University of Brighton aims to comply with requests for access to personal information as quickly as possible, but will ensure that it is provided within 40 days of receipt of the written application and, if appropriate, required fee. Should there be a good reason for delay, this will be explained in writing to the data subject making the request.

11.2 Examination Scripts

Students may also make a request using the above procedure to obtain a copy of their exam scripts once marks have been formally ratified and published. Note that if a Subject Access Request is received, the University need not provide examination marks until either the end of five months from receipt of the request or the end of 40 days after the day on which the results of the examination are announced, whichever is the earlier. Copies of the exam paper will not be provided.

12 Retention of data

12.1 Student records

In general, detailed information about students will be kept in the relevant school for a maximum of six years after they leave the University of Brighton. This will include:

- name and most recently notified address
- academic achievements, including marks for coursework
- copies of any reference written

After this period, information on what was studied by the student, what s/he achieved and any periods of intercalation will be available from Academic Services. Please refer to the Records Retention Schedules for relevant categories of record. All personal records will be disposed of securely to ensure there is no accidental disclosure to third parties.

Following completion of studies and to enable ongoing communication/interaction, student records are passed to the university's Alumni Association (run by the Philanthropy and Alumni Engagement department), unless students opt-out of this transfer when they enrol as a student. This means the primary point of contact for former students will be via the Alumni Association, in terms of updating details or seeking advice/support as a graduate. More information about the Alumni Association and what it offers former students can be found by visiting www.brighton.ac.uk/alumni

12.2 Staff records

In general, all information on a member of staff will be kept for six years after s/he has left the University. Some records, however, will be kept for much longer. This will include material necessary in respect of pensions, taxation, potential or current disputes or litigation regarding the employment. A full list of information with retention times is available from the Legal Adviser.

All personal records will be disposed of securely to ensure there is no accidental disclosure to third parties.

12.3 Personal information accessible via the internet

It may still be possible to access references to former staff and students through internet search engines after they have left the University of Brighton. This is unavoidable. As the information is already in the public domain, it is not subject to Data Protection legislation. However, should there be good cause to request its suppression, application should be made to the Legal Adviser in the first instance.

13 Conclusion

Compliance with the DPA is the responsibility of all members of the University of Brighton. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or access to University of Brighton facilities being withdrawn, or even a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be directed to the Legal Services Officer in the first instance.

Appendix 1

Data Protection Principles

Principle 1
Personal data must be processed fairly and lawfully

Principle 2
Personal data must be obtained only for one or more specified and lawful purposes and it must not be processed in a way that is incompatible with that purpose or those purposes

Principle 3
Personal data must be adequate, relevant and not excessive

Principle 4
Personal data must be accurate and, where necessary, kept up to date

Principle 5
Personal data must not be kept for longer than is necessary for its purpose

Principle 6
Personal data must be processed in accordance with the rights of the data subjects

Principle 7
Appropriate technical and organisational measures must be taken against accidental loss, destruction and damage to personal data

Principle 8
Personal data must not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data

Appendix 2

Glossary of Data Protection Terms

Data: in the context of the University of Brighton, information which is processed automatically/recorded with that intention or is recorded as part of a relevant filing system/with that intention.

Data Controller: the person/people who determine(s) the purposes for which, and the manner in which, personal information is to be processed and whose duty it is to ensure that the Data Protection Principles are applied. In the context of this institution the Data Controller is the University of Brighton.

Data Processor: external persons or agencies who process data on behalf of the university. This would include anyone responsible for the disposal of confidential waste.

Data Subject: any living individual who is the subject of personal information.

European Economic Area: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Gibralter, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, United Kingdom

Inaccurate Data: data which is incorrect or misleading as to a matter of fact.

Notification: entry on the public register maintained by the Information Commissioner's Office showing types and range of information being processed by the university.

Personal Data: information about a living individual who can be identified from that information or from other information that is in, or is likely to come into, the possession of the university.

Processing: obtaining, recording or holding information or carrying out any set of operations on it

Sensitive Personal Data: information as to the individual's

- racial or ethnic origin
- political beliefs
- religious beliefs or beliefs of a similar nature
- trade union membership
- physical or mental health or condition
- sexual life
- commission or alleged commission of any offence
- any proceedings for any offence committed or alleged, the disposal of such proceedings or the sentence of any court in such proceedings

Appendix 3a

Data Protection

Data Processing Notice - Staff

The University recognises that your personal privacy is important and it supports the principles of the Data Protection Act 1998. The information below explains what type of personal data is held, how and why it is processed and to whom it may be disclosed.

How the university uses your information

All personal information will be treated strictly in terms of the *Data Protection Act 1998*. It will be collected and used only as necessary in order to administer and manage the employment relationship, both during and after employment. It will be processed fairly, accurately and confidentially and will not be disclosed to others unlawfully. Information will be used for the purposes listed below by staffs that are responsible for those areas of work.

- Administration and management of appointment, employment, promotion and development, termination of employment and post employment requirements (e.g. pensions and references)
- Compliance with statutory requirements and statutory guidance, for example regarding equal opportunities, equal pay, work permits, and requests from benefits agencies
  Information necessary for the business of the University and provision of its services (e.g. courses).

Information on protection, monitoring and security of electronic information systems is contained in the *University of Brighton Information Systems Security and Information Interception Policy* and the *Conditions of Use of University of Brighton Computing Facilities, Including Networks*. Both documents are available on Staffcentral or from the Information Services Department.

Information for third parties

Anonymised data may be made available if requested to organisations seeking data for research or analysis of the University or the higher education sector. Such organisations include the Higher Education Statistics Agency (HESA) and the Higher Education Funding Council for England (HEFCE). Names and personal contact details will not be made available and precautions are taken to minimise the risk of identification of individuals from the data. relevant government departments to whom the university has a statutory obligation to release information - including the Higher Education Statistics Agency (HESA) and the Department for Business Innovation and Skills (BIS). Further information is contained in the HESA Fair Processing Notices: http://www.hesa.ac.uk/collection-notices.

Information may also be sent to staff about special discounts for products or services available to University staff.

Personal data will not otherwise be released for the marketing of products or services to staff.

Your responsibility

All staff are responsible for checking that any personal data that they provide to the University is accurate and up to date. They must inform the University of any changes to their data (e.g. change of name or address). All staff who process personal data are required to comply with the *Staff guidelines for handling of personal data*.

You are required to inform anyone whose contact details you have provided to the University for contacting in the case of an emergency that the information is being held and to ensure they are in agreement.

Further information

Further information regarding data protection, including your rights and responsibilities, can be found in the *Staff Handbook*, or your copy of *Signpost – a Staff Handbook summary* and in the following guidance documents available on Staffcentral:

Staff guidelines for handling of personal data

Conditions of Use of University of Brighton Computing Facilities including Networks

University of Brighton Information Systems Security and Information Interception Policy; Using Information Systems

University of Brighton Data Protection Policy

University of Brighton Information Systems Security and Information Interception Policy: Managing Information Systems (for anyone with responsibility for electronic information systems)

For the data protection policy of the Higher Education Statistics Agency (HESA)
http://www.hesa.ac.uk/dataprot/home.htm

For the data protection policy of the Higher Education Funding Council for England (HEFCE)
http://www.hefce.ac.uk/aboutus/cop/howdo/dpa/

Information is also available from the Legal Adviser, Andrew Wilson by e-mail or on extension 2404.

Appendix 3b

Data Processing Notice - Students

Data Protection

The University of Brighton is notified as a data controller with the Office of the Information Commissioner, and collects and processes information about students for various teaching, research and administrative purposes. All such activity is governed by the Data Protection Act 1998 and students are entitled to have access to the records held about them to ensure accuracy and fairness.

Purposes for which information is held include:

- general university administration requiring personal and academic details
- management of academic processes such as academic audits, examination boards and award of degrees
- the management of university residences, sport and leisure activities and university social events
- alumni operations, including fund-raising
- the provision of advice and support to students via, amongst others, the Registry, Student Services and the Accommodation Service
- internal research, including monitoring quality and performance.

The university, via academic Schools, the Registry and other ancillary departments, allows employees and agents of the university to access data on a strictly need-to-know basis. Student information is disclosed to a variety of third parties or their agents, notably:

- general university administration requiring personal and academic details
- management of academic processes such as academic audits, examination boards and award of degrees
- the management of university residences, sport and leisure activities and university social events
- the continuation of communications and support following completion of studies via the university's Alumni Association
- fundraising campaigns to enhance the University of Brighton experience for the future
- the provision of advice and support to students via, amongst others, Academic Services, Student Services and the Accommodation Service
- internal research, including monitoring quality and performance.
- The university, via academic Schools, Academic Services and other ancillary departments, allows employees and agents of the university to access data on a strictly need-to-know basis. Student information is disclosed to a variety of third parties or their agents, notably:

- students' sponsors (including LAs), the Student Loan Company, and funding and research councils
- Students' Union
- UKCAT (UK Clinical Aptitude Test Consortium)
- relevant government departments to whom the university has a statutory obligation to release information - including the Higher Education Statistics Agency (HESA) and the Department for Business Innovation and Skills (BIS). In the case of government departments, it will often be agents operating on their behalf to whom data will be disclosed and this data will be accessed and managed in line with the Data Protection Act. Further information is contained in the HESA Fair Processing Notices: http://www.hesa.ac.uk/collection-notices

- Council Tax Registration Officers
- current or potential employers of University of Brighton students
- current or potential providers of education to University of Brighton students (including placement providers)
- professional and statutory bodies
- for medical students, in the interests of public safety, (and in accordance with Tomorrow's Doctors), information pertinent to an individual's fitness to practise may be shared by Brighton and Sussex Medical School with training providers, employers, regulatory organisations and other medical schools.

The accuracy of personal information provided by students may also be checked by the university against relevant external sources. The university undertakes to maintain student data in secure conditions, and to process and disclose data only within the terms of its Data Protection notification. The details above indicate the nature of this notification but are not exhaustive. Please note that we are reliant on you for much of the data we hold: help us keep your record up-to-date by notifying us of any alterations to your address, personal details or course enrolments. The university's full data protection policy can be found at:

http://staffcentral.brighton.ac.uk/xpedio/groups/Public/documents/staffcentral/doc006938.pdf

Please contact the Legal Adviser, Mithras House, ext 2404, if you have any specific questions relating to Data Protection or for details of procedures relating to your rights as a data subject.

Appendix 4

Staff guidelines for the handling of personal data

1 Introduction

1.1 The Data Protection Act (1998) provides a framework to regulate the collection and use of personal information about living, identifiable individuals, to protect the privacy of the individual and discourage inappropriate use of personal information. These guidelines have been provided to ensure that all staff are aware of their obligations in relation to handling personal data and of the recommended procedures for doing so, whether the information is about staff or students.

1.2 "Personal Data" is defined as any information rel**a**ting to a living person and which can be identified as referring to him or her is included, whatever the format – electronic, paper, film, tape, text, still and moving image.

1.3 "Sensitive personal data" has a very specific meaning in terms of the Act: information relating to race; political opinion; religious belief; trade union membership; physical or mental health; sexuality; and any criminal history.

Documents with titles in italics can be accessed through Staffcentral.

2 Guidelines

2.1 Collection and use of personal data

Only information which is really necessary should be collected. Nothing should be either requested or recorded on the grounds that "it might come in useful". Neither should it be used for purposes inconsistent with those specified in the University's *Data Protection Policy or* Information Security Policy

Extra care should be taken in the handling and storage of sensitive personal data as defined above.

2.2 Storage

Precautions should be taken to prevent any unauthorised access to personal data. Any information relating to named individuals should be handled and stored securely:

- desks or filing cabinets should be locked
- computers should be secured
- password should be kept secret and secure – change them regularly
- data storage devices containing personal information should be kept safe
- papers should not be left out on desks or tables
- information on computer screens should not be accessible/visible to other than authorised users
- "sensitive" data should be secure and subject to very limited access.

Personal data should not be removed from the University or stored elsewhere unless such use is recognised and authorised. Off-site security must conform to University standards as outlined above.

To minimise the risk of personal data being mishandled, it is recommended that information be held in one file wherever possible, rather than being dispersed or duplicated in several places. For example, material concerning current students should be held on file in the School Office with the maintenance of separate files by tutors being avoided as far as is practicable and possible.

Data should not be held indefinitely. Please refer to the University's Records Retention Policy and Schedules.

2.3 Cloud Services

Cloud-based services, such as Dropbox, Google Apps, and Microsoft OneDrive, have become increasingly common for both data and applications. Because of security issues and concerns that data may be processed outside the EEA (in breach of "Principle 8" – see Appendix 1), personal data* must only be stored on centrally provided or supported cloud services. Whilst staff and students may choose to use externally provided cloud services this must never be used for the storage or processing of personal data.

2.4 Disclosure

No information should be given to any third party without permission of the member of staff or student. This includes parents or other relations, partners, friends, colleagues, fellow students. For more detail and explanation of this area, including circumstances where disclosure is permitted, reference should be made to *Guidelines for the disclosure of personal student data (Appendix 5 of the Data Protection Policy).*

In particular, it should be noted that the police have certain powers under the act to access personal information which we hold. This is not generally an automatic right (subject to certain exceptions such as "RIPA"), however, and must be in relation to investigation/detection of a crime and/or apprehension of an offender. Extreme care must be taken to establish the identity of the caller and no information should be divulged without an official written communication showing crime number and the name, rank and badge number of the investigating officer. Such cases must always be referred to the Legal Adviser, Andrew Wilson on ext.2404.
If you are contacted concerning Child Protection, CRB, Safeguarding or a matter concerning an issue of conduct in a placement at a school or hospital please refer this to either the Legal Services Officer or the Registrar and Secretary.

2.5 Providing references

When supplying a reference, it is always safest to assume (whether or not it is given in confidence) that the subject will have the right to read it. Although access to personal references does not have to be provided by the writer, in most cases the subject will be able to request a copy through the recipient. Information should be factual and verifiable with unsubstantiated opinion being avoided.

2.6 Disposal

Records must be disposed of securely through shredding or incineration to ensure no accidental disclosure to any third parties. Particular care and caution must be exercised in the reuse and disposal of computers. University guidance on this is available in *University of Brighton Information Systems Security and Information Interception Policy: Managing Information Systems.*

3 Further information

For further details please refer to the *Data Protection Policy* which includes Appendices covering both Staff and Student Data.

Please refer any queries to the University's Legal Adviser, Andrew Wilson, Mithras House, extension 2404.

Appendix 5

Data Protection: Guidelines for the Disclosure of Student Data

1 Introduction

Since the University of Brighton receives regular requests for information on students, both past and current, selected guidance is reproduced here. Please do not hesitate to contact the Legal Adviser (Andrew Wilson ext 2404) should you need any further information or explanation. The main thing to remember is that, according to the Data Protection Act 1998 (DPA), the circumstance under which any personal information can be disclosed without the authorisation of the individual are fairly limited.

2 Disclosure synopsis

The list below shows who might request student information from the University either as a regular or ad hoc occurrence. Please note:

- any request accompanied by a valid Court Order **must** be dealt with promptly and the required information supplied (Appendix 2)
- where noted, individual requests received from organisations/bodies listed below must be verifiable. They must be made in writing on official headed paper and should ideally cite the relevant DPA exemption or other legislation which authorises the University to release the information.
- where noted, details of any such release should be reported to the Legal Adviser for entry in the institutional Exceptional Disclosures Log

2.1 Exceptional circumstances

Confidentiality may have to be breached if there is a danger that

- the student may harm him/herself
- the student may harm other persons
- the student's life or health or safety may be threatened

2.2 Families

The University has an obligation NOT to provide information to family members without consent as students are private individuals. Although staff may come under pressure to discuss students' cases with parents, it is essential that personal information is not disclosed without the written consent of the student involved. Institutional procedures, however, may be discussed freely with anyone. Thus it is possible to explain to a parent what, *in principle*, happens when a student must retake examinations, spend a year on industrial placement, etc but not to divulge the specific circumstances of an individual's case without the agreement of that student.

2.3 The Police/Court Order

Disclosures to the Police are not compulsory except where the institution is served with a Court Order. In such cases please advise the Legal Adviser or Registrar and Secretary immediately. The DPA allows disclosure where data is requested for "the prevention or detection of crime" and "the apprehension or prosecution of offenders". Disclosures should be made only in cases where the Police confirm that they wish to contact a named individual about a named criminal investigation, regardless of whether that individual is suspect or witness, *and where we are reasonably satisfied that failure to release would prejudice the investigation*. Information should be provided only on receipt of written confirmation with the signature and badge number of the investigating officer. This should always include a statement confirming that the information requested is required for the purposes covered in Section 29. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.4 Government agencies

2.4.1 Her Majesty's Revenue and Customs (HMRC)

Disclosures should be made when an official written application is received from HMRC in relation to the collection of tax or duty. The relevant DPA exemption, normally section 29, should be quoted. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.4.2 Home Office/Home Office Border and Immigration Agency

There is a statutory obligation to co-operate when enquiries are received from the Home Office. The request should be made in writing on official paper and it is best practice for the relevant exemption to be quoted. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.4.3 Child Support Agency (CSA)

There is a statutory obligation to co-operate when enquiries are received from the CSA. The request should be made in writing on official paper and it is best practice for the relevant exemption to be quoted. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.4.4 Financial Services Agency (FSA)

There is a statutory obligation to co-operate when enquiries are received from the FSA. The request should be made in writing on official paper and it is best practice for the relevant exemption to be quoted. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.4.5 Department for Work and Pensions (DWP)/Jobcentreplus

In cases where an officer of the DWP suspects an individual of benefit fraud, statutory powers are available to them to *require* the University to provide data on one or more named individuals. An explicit written statement should be obtained from the relevant authorised Officer explaining the context of the request. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.4.6 Health and Safety Executive (HSE)

In cases of accidental injury, such as occurring to a student in the science laboratory, the University is legally obliged to report details of the incident and basic personal details of those injured to the HSE. This should be done through the Head of Health and Safety, Alan Cowen.

2.4.7 Department of Health/Environmental Health Officers

In cases of notifiable disease amongst students, the University may be approached by Environmental Health Officers, acting on behalf of a local Medical Officer for Health, requesting information about the student who is suffering the illness and/or those who are believed to have been in close contact with him/her. There is a statutory obligation on institutions to disclose in cases of notifiable disease. Where the disease is serious but not notifiable, the University may choose to disclose to protect the vital interests of the individual and this would be permissible under DPA. In such cases, the University should disclose only basic details such as name and contact address. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.4.8 Environment Agency

Under normal circumstances the University should not pass personal information to the Environment Agency. However, in cases of actual or potential breach of the Agency's regulations, such as inappropriate disposal of radioactive material, disclosure may be valid. Any request for information should be reported to Andrew Wilson, Legal Adviser, ext: 2404.

2.5 Higher education agencies

2.5.1 Higher Education Funding Council for England (HEFCE) and agents such as Higher Education Statistics Agency (HESA) and HEFCE auditors

The University is required by law to disclose information to the Higher Education Funding Council for England on request. This includes the incidental disclosure of student data during visits by academic or other auditors appointed by the Funding Council. Disclosures may also be made to agents of the Funding Council. There is an explanatory statement in the Student Handbook to ensure full awareness.

2.5.2 Quality Assurance Agency for Higher Education (QAA)

In the course of normal and legitimate activity, it is possible that student information may be disclosed to the QAA.

2.5.3 UCAS

As applicants are made aware by UCAS when they first submit their details that information will be passed between them and the University, relevant data may be shared freely with UCAS as the need arises

2.6 University-related

2.6.1 University insurers

In cases of accidents occurring within institutional property, the University may need to release the details of the accident to its insurers. This may involve disclosure of student details, notably in cases where a student has suffered injury and may be in a position to claim damages.

2.6.2 Work placement sites

In cases where students undertake industrial and Health Service placements as part of a course, there will, of necessity, be a limited flow of student information between the University and placement sites. Students should be notified of this before their placement begins. Care must be taken to restrict the information to that which is essential for the administration of the placement.

2.6.3 Solicitors acting on behalf of the University

The University may, without subject consent, release information to its solicitor(s) if that information is relevant to any case on which the institution is seeking legal advice. Section 35(2) states that the Act's non-disclosure provisions are waived for the purpose of obtaining legal advice.

2.6.4 Landlords of University-managed properties

Where the University manages residences on behalf of landlords, acting effectively as a letting agent, there is no direct contractual or other formal relationship between landlord and student. Should a landlord wish to be given the details of the student(s) resident in his/her property, then such disclosures can only be made with the consent of the student(s) involved.

2.6.5 Debt collection agencies acting for the University

In cases of bad debt, the University may refer students to debt collection agencies. Such disclosure can be justified in terms of the pursuit of the institution's legitimate interests. No "sensitive data" as expressed in DPA (Appendix 1) should be passed to any debt agency. Students should be informed of this possibility, at the commencement of any debt review procedures.

2.6.6 Mentors, alumni representatives and other overseas representatives

The University operates a network of former students and other agents who are available to give advice to applicants, particularly overseas applicants, about the institution. Applicants must give consent for their details to be passed to such agents and they should not receive *unsolicited* calls from representatives.
The same consent must be sought from potential or new students before their details are communicated to existing students who are to act as mentors.

2.6.7 Prize-givers

In most cases where external bodies, such as private companies, professional bodies, and charities, fund prizes to be given to students who attain high standards, the organisations will wish to see the details of those who have received their prizes. The University should, therefore, make prize-winners aware that acceptance of the prize will indicate consent for details to be disclosed to the prize-giver. Only the minimum possible - name and a general indication of performance - should be disclosed.

2.6.8 External auditors

The University is required by its own statutes to appoint external financial auditors. It is acceptable that such auditors *will* inevitably see student data during the course of their investigations.

2.6.9 Professional bodies

The university should ensure that, in cases where particular degree schemes lead to professional recognition, accreditation or exemption, students on such courses are told at point of registration that their final result, including any failures, will be communicated to the relevant professional body. Should a professional body make an ad hoc approach for personal details of students with qualifications in a particular academic discipline, such enquiries can only be answered with the consent of the student(s) involved.

2.6.10 Sponsors/sponsoring bodies

The University has an obligation NOT to provide information to sponsors without consent. Any arrangements students have made regarding the payment of their fees does not alter the fact that this is an arrangement between the student and the body funding the student, not between the University and the body. Consent for such disclosure may be proven in two ways:

- Written permission from the student to provide the sponsor with any requested information about such things as attendance and results
- The verified existence of a contractual arrangement between the student and the sponsor which permits the disclosure of specified information

2.6.11 Student Loans Company (SLC)

The SLC provides loans and, in some cases, fee payments for undergraduate students. Students who are in receipt of such funding sign a formal agreement with the SLC regarding the financing of their studies, a contract which permits disclosure of personal information by the University as necessary.

2.7 Local authority

2.7.1 Local Authorities

Local Authorities assess undergraduate student eligibility for fee and loan payments, operating on behalf of the **Department for Business, Innovation and Skills.** Whilst the first assessment process requires no disclosure of information from the University to a Local Authority, the local Authority will require confirmation that students have taken up their place and/or that they are still in attendance. The University is under statutory obligation to make such disclosures, although information provided should be limited to bare facts of name and attendance but not results.

2.7.2 Census

Census officers have no statutory right to ask the University to provide student data. The University should co-operate with the distribution of Census forms as far as is possible, but personal information should not be released directly to Census officers without prior permission from the student(s) involved.

2.7.3 Council Tax Registration Officers

Student data *may* be disclosed to Council Tax Registration Officers as necessary, even without consent. The requirement is that there be reasonable grounds for believing that a failure to disclose would be likely to prejudice the collection or assessment of any tax or duty. The request must be made in writing and specify the exact provisions under which the request is made, normally section 29. Any release should be reported to the Legal Services Officer for entry in the institutional Exceptional Disclosures Log. Any release should be reported to the Legal Services Officer for entry in the institutional Exceptional Disclosures Log.

2.7.4 Electoral Registration Officers

Electoral Registration Officers have certain powers to require the provision of student information for the purposes of maintaining registers of parliamentary and local government electors. If approached by an Electoral Registration Officer for information about students, the University should check why the data is required and under what powers. If satisfied with this, the disclosure can be made. However students should be informed of the disclosure.

2.8 Other

2.8.1 Survey/research organisations

The University may be approached, from time to time, by survey and research organisations, or others conducting research, who wish to be provided with student information or contact details for a sample of the student body. The University *must* seek informed consent from any student whose details might be disclosed in this context.

2.8.2 Other educational establishments

The University may be asked for information about current or former students by other educational establishments. Typically, this occurs when a former student wishes to be admitted to a course elsewhere and has freely provided details of prior study. The information released should be the minimum relevant to the request – usually attendance and award details although classification and module marks may also be relevant in certain circumstances. Response should only be made to requests received in writing.
Requests for information from institutions formerly attended by the student should not normally be met, unless either the student has authorised the disclosure or the other institution can provide verifiable justification under the DPA.

2.8.3 Employers and Recruitment Agencies

The University may be asked for information about existing or former students by current or potential employers and recruitment agencies. Typically, this occurs when such a student applies for a job. As the student has freely supplied details of previous or ongoing study, relevant information may be provided.

2.8.4 Overseas institutions

In cases where there are formal exchange links between the University and overseas HEIs or equivalent bodies, there will, of necessity, be a limited flow of student data between these sites. In cases where the exchange institution is based outside the EEA, such disclosure will usually require consent from students, sought before their exchange begins. Disclosure to institutions inside the EEA will not need consent.

2.8.5 Solicitors acting on behalf of other persons/bodies

The DPA's non-disclosure provisions are waived for the purpose of "or in connection with legal proceedings…or is otherwise necessary for…establishing, exercising or defending legal rights". In cases where the University is approached by solicitors or others engaged in a Court case, it is worth noting that there is no *compulsion* to disclose, just because the law gives dispensation to do so. In cases where the institution has no direct involvement in the case, it may be advisable not to disclose anything without the consent of the student concerned.

2.8.6 Journalists

Although there is an exemption from many of the provisions of the Act for the processing of personal data for the purposes of journalism, this does **not** allow for the disclosure of personal data to journalists by University staff.

2.8.7 National Health Service (NHS) Fraud Investigators

Official requests received in writing and which cite the relevant DPA exemption to permit disclosure should normally be met.

2.8.8 Embassies/High Commissions

Enquiries should be treated with extreme caution and nothing disclosed without the express consent of the relevant student. The extent of the relationship is a matter for the student, not the University, to determine.

Appendix 6

Use of Staff Images

1. Introduction

1.1 This policy has been written to ensure that the University of Brighton complies with legal requirements in the use of staff images. For more information please consult the Data Protection Policy.

1.2 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 University of Brighton.

1.3 Any questions about this policy, or the Data Protection policy, should be directed to the Legal Adviser.

2. Publication of information by the University of Brighton

2.1 The University of Brighton is committed to openness and accessibility in the provision of information for all aspects of its work, having due regard to issues of efficiency, legality, security and confidentiality. Please refer to section 6 of the Data Protection Policy.

3. Online Image Publishing Consent

3.1 Staff are given the opportunity to indicate their consent or to withhold their consent to online publishing of their photograph by completing the "opt in" boxes on their Staffcentral Profile Page. Staff are invited to 'opt in' to two choices:

i. Consent to the University using their image for information services and internal communication ('non-public') purposes (see 4 below).
ii. Consent to the University using their image for information services and external communication ('public') purposes (see 5 below).

3.2 Once consent has been given for each of these options, it is not required that an individual be contacted for specific instances. Individuals may however be contacted to enquire about the suitability of an image.

3.3 Staff may choose to opt out at any time save that the University reserves the right to use images for security and identification purposes.

4. Use of staff photos for information services and internal communication ('non-public') purposes

4.1 In this context 'non-public' refers to areas of Staffcentral and Student Central that can only be accessed by means of a login and University of Brighton computer account.

4.2 The University of Brighton is committed to improving information services and internal communications. Examples of this are – but not restricted to:

i. The use of staff profile photos on the internal 'staff central' intranet contacts directory.
ii. The use of staff profile photos on the internal 'student central' intranet.
iii. The use of staff photos to illustrate internal communications work on any communication channel (for example staff news stories on the intranet)
iv. The use of staff photographs for university information services, internal communications and internal social media channels as they develop.

4.3 Individuals will often be contacted for specific circumstances where it would be good practice to offer a choice of photo, for example use of an individual's photo on the intranet homepage (e.g. for use in news stories on staffcentral).

5. Use of staff photos for external communication ('public') purposes

5.1 'External' or 'public' purposes in this context means the display of staff photographs on the University website or any part of Staffcentral visible by members of the public without the need to login.

5.2 The University of Brighton is committed to improving information services and external communications. Examples of this are – but not restricted to:

i. The use of staff photographs to accompany individual contact details on the university website
ii. The use of staff photographs to illustrate external communications work on any communication channel (for example news stories on the university website or press releases)
iii. The display of staff photos on walls, for example in a school foyer.
iv. The use of staff photographs for university information services, external communications and social media channels as they develop.

5.3 Individuals will often be contacted for specific circumstances where it would be good practice to offer a choice of photo, for example use of an individual's photo to be attached to a press release.

6. Suitability of images

6.1 Staff photos must not potentially offend others, or show incriminating or embarrassing behaviour. Photos must not undermine the University's positive reputation and values.

6.2 Any staff member may be requested to remove a personal photo with a more suitable image.

AJ/avw 25.3.14

Appendix 7
Policy on Personal Data Security Breach

1. Introduction

The University of Brighton is registered with the Information Commissioner as a "Data Controller" i.e. an organisation that processes personal data. We are therefore required to take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. This policy is intended as one such measure to provide guidance on how to report and investigate a data security breach. It is based upon and incorporates the guidance issued by the Information Commissioner.

2. Data Protection Principles

All users of personal data have a responsibility to ensure that they process such data in accordance with the Data Protection Action 1998 and in particular in accordance with the Eight Data Protection Principles. The Principles state that personal data must be:

1. Fairly and lawfully processed;
2. Processed for limited purposes;
3. Adequate, relevant and not excessive;
4. Accurate;
5. Not kept for longer than is necessary;
6. Processed in line with the individual's rights;
7. Secure; and
8. Not transferred to countries outside the EEA without adequate protection.

For full details please refer to the University Data Protection Policy and Appendices.

3. Liability for Personal Data Breach

Any breach of the Data Protection Act may render the University liable to legal action by the Information Commissioner and may also amount to a disciplinary offence. All data breaches, whether accidental or not, should be reported to the Legal Adviser so that appropriate action can be taken, where possible to contain the breach or to advise any individuals likely to suffer distress or inconvenience as a result.

4. Procedure

A data security breach can happen for a number of reasons:

- 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
- 'Blagging' offences where information is obtained by deceiving the organisation who holds it.

However the breach has occurred, there are four important elements to any breach management plan:

1. Containment and recovery
2. Assessment of ongoing risk
3. Notification of breach
4. Evaluation and response

Investigation of personal data security breaches includes not only a damage limitation exercise but also a recovery plan. If the breach is not serious, the Legal Adviser, in consultation with line management for the area responsible for the breach, will determine what action to take and who needs to be aware of the breach. The Information Commissioner does not define the term "serious breach" but the overriding consideration is determining the potential harm, which can occur, e.g. exposure to identity theft. The extent of harm depends on both the volume of personal data released and the sensitivity of the data. If the Legal Adviser considers the breach to be serious, it will be notified to the Registrar and Secretary, who will appoint a member of staff to lead the investigation into the breach, ensuring that adequate resources are assigned to this task. The investigation will involve staff from school or department where the breach occurred and potentially also from Information Services, Human Resources, and Marketing and Communications (Press Office).

5. Notification of the Breach

An important element in managing a breach is informing the individuals whose data has been compromised. Notification will enable individuals affected by the breach to take steps to mitigate the risks and to allow the appropriate regulatory bodies to provide advice, deal with complaints and perform their functions. In deliberating the most appropriate way to notify those affected, the urgency of the situation and the security of the medium are key considerations. Notification should include:

1. A description of the data involved;
2. Details of how and when the breach occurred;
3. What action has already been taken to respond to the risks posed by the breach; and
4. Contact details for further information.

Consideration should be given to notifying third parties such as the police, insurers, bank or credit card companies, and the trade unions. Though not a statutory requirement, the Information Commissioner believes that serious breaches should be brought to his attention. Notification to the ICO should include:

1. The type of information and number of records;
2. Circumstances of the loss, release or corruption;
3. Action taken to mitigate effect on individuals;
4. If individuals have been informed and whether any other organizations have been informed;
5. Details of the security measures in place and, where appropriate, details of the security procedures in place at the time the breach occurred;
6. Remedial action taken to prevent future occurrences; and
7. If the media are aware of the breach so that ICO can manage any increase in enquiries from the public.

The Press Office should be contacted about preparing and issuing a press release as necessary. When informing the media, it is useful to report whether or not the Information Commissioner's Office has been informed and what action is being taken (note that the ICO will not normally tell the media or other parties about a breach).

6. The University's Response

It is important not only to investigate the causes of any data breach but also to consider the effectiveness of the University's response in case there are systemic or ongoing problems e.g. lack of clear allocation of responsibility, inadequate policies or procedures. Monitoring of staff awareness of security issues may reveal gaps that can be filled through tailored advice or training. Risks will arise when sharing data with or disclosing data to others. The storing or transmission of personal data on portable or mobile devices is a weak point in security measures if encryption is not employed. Where the breach is serious, a written report will be prepared for the Registrar and Secretary after the investigation is complete and mitigating action taken. Any disciplinary action resulting from the investigation will fall under the normal agreed disciplinary procedures.

APPENDIX 7 cont.

ICO Guidance on Data Security Breach Management (Abridged)

1. Containment and recovery

Data security breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the business such as IT, HR and legal and in some cases contact with external stakeholders and suppliers. Consider the following:

- 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 back up 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.
The following points are also likely to be helpful in making this assessment:

- What type of data is involved?
- How sensitive is it? Remember that some data is sensitive because of its very personal nature (health 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. Consider the following:

- 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, you should inform the ICO.
- 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 2 million 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. ICO will not normally tell the media or other third parties about a breach notified to us, but we may advise you to do so.
The ICO has produced guidance for organisations on the information we expect to receive as part of a breach notification and on what organisations can expect from us on receipt of their notification. This guidance is available on our website:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/principle_7.aspx

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 you:

- Make sure you know 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

AVW 15.5.15 version 5