PERSONAL DATA AT THE UNIVERSITY OF SUNDERLAND

GUIDANCE NOTE FOR STAFF

Document classification: Public

Version 1.0
December 2013

The University's policies for handling information, and particularly personal data, are set out in these documents, available on Docushare:

Overarching Information Governance Policy (IG 001)
Data Protection Policy (IG 002)

The Overarching Information Governance Policy also provides a guide to other relevant policies.

This guide is intended to provide practical help for staff in implementing the policies. Further help can be obtained from the Data Protection Officer in Legal, Governance and Business Assurance, 4th Floor, Edinburgh Building, City Campus:

Dataprotection@sunderland.ac.uk
0191 515 2508

Contents

Glossary
1. Introduction
2. Principles
    2.1 Being fair
    2.2 Being lawful
3. Getting personal data right
4. Security
. Rights of the data subject
    5.1 Seeing their own data
        5.1.1 Routine requests
        5.1.2 More complex subject access requests
    5.2 Asking us to stop using their data
6. Using information within the University
    6.1 Routine business
    6.2 Unusual or new activities
    6.3 Research
7. Providing personal data to third parties
    7.1 One-off inquiries
    7.2 Freedom of information requests
    7.3 Giving information to contractors
    7.4 Sharing information with partners
8. Transferring data outside the EEA
9. Data breaches
10. Staff's own personal data

Appendices

A. Useful contacts
B. Fair Processing Notice for Students
C. Fair Processing Notice for Staff
D. Single page advice note

Glossary

Personal data Information about an identifiable, living individual. Names, addresses, photographs, grades, and notes of an individual's opinions are all examples of personal data

Data subject The person the information is about

Data processing Handling information in any way, including obtaining it, storing it, keeping it, analysing it, passing it around, publishing it and deleting or destroying it

Fair Processing Notice also known as a **Privacy Notice**. This sets out the purposes for which the University will use personal data, and who might have access to it. There are general Fair Processing Notices for both students and staff, covering the University's main activities, but particular exercises (eg a survey) may also require specific Fair Processing Notices

Subject access request A request by an individual to see the data held about them

1. Introduction

The University handles a lot of information about people – students, staff and others. Using that information effectively is an important part of our business, but we also have a responsibility to keep people's information safe, secure and convenient. Everyone who works for the University shares that responsibility.

If we get it wrong:

- There can be negative consequences for the individuals concerned
- There can be damage to the University's reputation
- Penalties can be imposed on the University by the Information Commissioner, including fines of up to £500,000.

All sorts of personal information are covered by this guide. It particularly focuses on the legal protections for information about an identifiable, living individual. Names, addresses, photographs, grades, and notes of an individual's opinions are all examples of personal data, and they are protected however the University stores them – on an electronic database, in a filing cabinet, or even in a handwritten note stuck to your telephone.

2. Principles

The most basic principle- the first principle laid down by the Data Protection Act 1998 - is that all our handling of personal information (or "processing" of "personal data") must be FAIR and LAWFUL.

2.1 Being fair

Fairness is a matter of judgement. If you have any doubt about whether or not it is fair to make use of personal data, try working through these questions:

What would the data subject expect us to do?
Except in a very few cases allowed by law, we should always tell people what use we are making of their personal data. The University publishes a Fair Processing Notice in the Student Handbook every year, which sets out the routine uses to which we put students' personal data. There is an equivalent notice for staff personal data on the Human Resources web-site. If what you want to do is covered by these notices, it is likely to be fair to do it.

Would using the information cause any unjustified harm to the data subject?
This is not always obvious. It pays to be cautious. For example, if a parent asks for the address of his or her son or daughter, we generally have no way of knowing whether or not they are estranged – offer to take a message instead, or get the student's permission first.

On the other hand, it may sometimes be fair to use information even if there is some harm to the data subject – for a disciplinary procedure, for example – provided this is justified.

Would failing to use the information cause any unjustified harm to the data subject?
Data protection is often thought to be about not making use of personal information, but the requirement to be fair will often point the other way. For example, if an international

student is being held at the airport by Home Office border officials, it would probably cause the student harm if we did not reveal that he or she had a place at the University.

2.2 Being lawful

Handling personal information may be affected by common law duty of confidence and Article 8 of the European Convention on Human Rights (the right to privacy) among others, but the main legal framework is provided by the Data Protection Act 1998.

The Data Protection Act sets out eight principles for using personal data:

1. As we have seen, it must be done fairly and lawfully. Each use of personal information must meet at least one specified condition for processing, discussed in the rest of this section.

2. Personal information must be used for a specified purpose and not reused for an incompatible purpose. For example, if we have told University alumni that we are collecting their e-mail addresses to keep them in touch with developments at the University, we could not then sell that contact list to an internet marketing company.

3. Information must be adequate, relevant, and not excessive for the purpose for which it is being used.

4. Information must be accurate and, where appropriate, up-to-date.

5. Information must not be kept longer than necessary for the purpose for which it is being used (but allow for the possibility of complaints or legal action).

6. We must respect the rights of the data subject to see their own data or stop us from using it in some circumstances (see section 4 below).

7. There must be appropriate technical and organisational measures for security (see section 3 below)

8. Personal data must not be transferred outside the European Economic Area (EEA – the EU plus some affiliates) unless strict conditions are met. This applies equally to, for example, placing documents on a server located in the USA, taking a memory stick to a conference in India, or setting up a recruitment arrangement with a partner in China (see section 7 below).

Any use of most personal data – anything that is not classed as "sensitive" – must meet at least one of these conditions:

- The subject has freely consented (and may withdraw consent at any point)
- It is necessary to carry out a contract (or prospective contract) with the data subject
- It is necessary to meet some other legal obligation
- It is in the vital interests of subject (literally life-or-death)
- It is necessary for the administration of justice & other public functions (eg if we are approached for information by the police or the courts)
- It is necessary to meet the "legitimate interests" of data controller – unless it causes unwarranted prejudice to the interests of subject. The Fair Processing Notices are good guides to what the University's legitimate interests require.

Some information is classed by the Data Protection Act as "Sensitive Personal Data". This is information about someone's:

- Race or ethnicity
- Political opinions
- Religious beliefs (or similar)
- Trade Union membership
- Mental or physical health
- Sex life
- Offences, alleged offences, court proceedings, or sentences.

Any use of sensitive personal data must meet at least one of the conditions set out above and one of these conditions as well:

- The subject has freely given explicit consent, which may be withdrawn at any time. The meaning of "explicit" is unclear, but it is generally sensible to get consent in writing.
- It is necessary to meet a legal obligation relating to employment.
- It is necessary to protect the vital interests of subject or third party (again, this is literally life or death).
- The data has already made public by the data subject.
- It is necessary for legal proceedings.
- It is necessary for the administration of justice or police purposes.
- It is necessary for medical purposes, and is being used by a health professional.
- It is necessary for equality monitoring.
- Or, when "in the substantial public interest", it is necessary for
    - The prevention or detection of crime
    - Protecting the public from malpractice or mismanagement
    - Providing confidential counselling
    - Some insurance and pension functions
    - Research.

Whether or not something is "in the substantial public interest" is obviously arguable, so it is best, if possible, to rely on one of the other conditions.

The definition of "sensitive" personal data can have unexpected effects. For example, information about sick leave, early departure from work for religious observance or time off for trade union activities, is classed as "sensitive": if asked about such absence, unless the individual has agreed you can be specific, just say that they are away from work without saying why.

On the other hand, information about personal finances is not classed as "sensitive" by the Act, but the University normally treats it that way for security purposes.

3. Getting personal data right

The Data Protection Act 1998 tells us that personal data must be

- adequate, relevant, and not excessive for the purpose for which it is being used
- accurate and, where appropriate, up-to-date
- not kept longer than necessary for the purpose for which it is being used.

The key is always to refer back to the purpose for which the data is being used. You should only collect, store, use, disclose or publish personal information that is necessary for that particular

purpose. If someone has made a legitimate request for information, give them only that, not other information which you think might interest them.

Beware of simply reusing old databases, spreadsheets or lists, as they are likely to contain information that is irrelevant or excessive for the new purpose, and may well be out-of-date too. They may also be missing some of the information needed for this particular purpose.

It will often be necessary to keep some information after you have finished using it yourself (for example, to reply to a letter or to determine a grade). This is to allow for historical archives, audit, complaints and even the possibility of legal action. The University uses the record retention schedules published by JISC, and you should consult these to find the appropriate periods to keep different kinds of information or document. At the time of writing, they are posted at http://bcs.jiscinfonet.ac.uk/he/ .

4. Security

The most common cause of fines and enforcement notices for breaches of the Data Protection Act is a failure to keep personal information secure. Frequent problems include:

- E-mails or letters sent to the wrong address
- Unintended attachments, resulting from forwarding e-mails or chosing the wrong document from a file
- Hidden data – for example in spreadsheets
- Paper documents being left in pubs, taxis or, old buildings
- Data being shared with partners who don't keep it secure
- Unencrypted laptops or memory sticks being lost or stolen. We can expect similar problems from unencrypted data being stored in the Cloud.

So that everyone handling it realises the importance of keeping it secure, all personal data should be marked "Confidential", and all sensitive personal data should be marked "Sensitive".

The actual measures you take should be proportionate to the risks that might arise if data was misused or leaked. The University's policy on Information Classification suggests the following:

Keeping paper records secure

- Use locked cabinets
- Use an approved third party courier
- Use sealed envelopes not transit envelopes
- Use secure disposal

Keeping electronic records secure

- Use encryption – particularly if you are using mobile devices (smart phones, tablets, laptops), memory sticks or Cloud storage
- Apply password protection
- Use SFTP (Secure file transfer protocol)
- Use secure file stores
- Use secure disposal
- Set appropriate access rights and levels of privileges for different staff.

Keys, passwords and access rights should be changed and updated from time to time as staff change roles. Information should only be available or passed on even to other University staff if it is necessary.

In addition, be careful about using speakerphones and about reading documents in public. Social media (such as Facebook, Twitter and LinkedIn) should not be treated as secure, whatever the privacy settings available.

5. Rights of the data subject

5.1 Seeing their own data

People have the right to see any information we hold about them, except in some very tightly constrained circumstances (for example, if a medical professional has ruled that it would be harmful for them to see it, or if it is part of an investigation of a crime).

In the Data Protection Act, a request by an individual to see the information held about them by an organisation is called a "Subject Access Request". We have to reply to a Subject Access Request within 40 (calendar) days. The Act allows organisations to make a charge of up to £10, but the University does not at present charge anything (while reserving the right to do so in future).

There is an exemption from the 40-day deadline if it would result in revealing exam results before they are due to be published.

It is unlikely that people will specify that they are making a Subject Access Request. They may call it something else (for example, a Freedom of Information request, although FOI does not generally apply to personal data), but it should still be treated the same way.

5.1.1 Routine requests

Many requests for information are straightforward and can be dealt with on the spot. For example, if a student with a room in one of the halls of residence wants to know how much rent he or she owes, it is only necessary to check the student's identity (perhaps by asking to see a Campus Card, if the student isn't personally known to the member of staff they have approached), and the information can be handed over.

5.1.2 More complex subject access requests

Sometimes requests are more complicated, perhaps because:

- They involve a lot of data;
- They involve data held by different parts of the University;
- They involve other people's personal data too;
- It isn't clear what information they are asking for.

Such requests should be referred to the Data Protection Officer (Dataprotection@sunderland.ac.uk) who will liaise with the person making the request to clarify any issues and co-ordinate a reply on behalf of the University.

5.2 Asking us to stop using their data

People have a general right to ask us to stop using information about them for particular purposes if it would cause them unwarranted, substantial damage or distress. We have to consider these requests and reply within 21 (calendar) days either agreeing to stop, or explaining why we are continuing to use the information. This might be for one of these reasons:

- Because we disagree that there will be substantial damage or distress, or that it is unwarranted
- Because it is necessary to carry out a contract (or prospective contract) with the data subject
- Because it is necessary to meet some other legal obligation
- Because it is in the vital interests of subject (literally life-or-death).

People have the absolute right to stop us using their personal data for **marketing** purposes. "Marketing" is very broadly defined as anything intended to influence someone's opinion. If anyone asks us to do so, we must stop. If the request is a general one – not just that they do not want to hear from you or about the things you have sent them, but a request not to hear from the University at all, inform the Data Protection Officer. If someone asks to come off one of your mailing lists, keep a record so that they are not accidentally added back again (this is sometimes called a "suppression list").

People also have the right to stop us taking entirely **automated decisions** about them. This is aimed mostly at groups such as credit rating agencies, whose ratings are mostly generated by computer programmes alone, and is unlikely to affect the University much. But if such a request is received, and no human has been involved in taking decisions about the individual, an appropriate member of staff must review the decision and be involved in decision-making about that individual in future.

6**. Using information within the University**

6.1 Routine business

Most routine uses of personal information within the University are already fair and lawful, but it is worth checking from time to time against the principles and conditions set out in section 2. In general, if your activities are covered by the Fair Processing Notices issued to staff and students, you are probably OK. If not, contact the Data Protection Officer (Dataprotection@sunderland.ac.uk).

You should also review security from time to time (section 3).

6.2 Unusual or new activities

The Data Protection Act is not intended to prevent organisations from using personal data provided they do so responsibly, but it may mean that some systems and ways of doing things are more likely to be fair and lawful than others. It is therefore worth taking data protection needs into account right from the start of any project that involves using personal data.

Questions worth asking include:

- What personal information is needed for what purpose?
- Is any of it "sensitive" personal data?
- How will the information flow? Who needs to see it and when? Are there any external partners involved?

- What risks are there that information might be misused (including using inadequate, irrelevant or inaccurate data) or wrongly disclosed? What would be the consequences if that happened?
- What controls are needed to counter those risks?

In the case of a small project, this might be a quick paper exercise by the responsible member of staff, consulting this guide for assistance in identifying risks and controls. In the case of a large project, involving large amounts of personal data, a more formal and structured exercise, involving widespread consultation, may be necessary. You can consult the Assurance Manager (Information Governance) at ba@sunderland.ac.uk or the Data Protection Officer for guidance.

In many cases, it may be necessary to contact the people whose personal data is being used in the project with a short Fair Processing Notice, either to let them know what is going on, or to ask for their consent.

6.3 Research

There are two exemptions from the principles set out at 2.2 above for research, historical or statistical purposes:

- Whatever the purpose for which personal data was originally collected, it can also be used for these purposes.
- Personal data used for research, historical or statistical purposes can be kept indefinitely.

These exemptions only apply if:
Personal data is not used for decisions about individuals.

- Using their personal data for research causes no substantial damage or distress to an individual.
- The published results of the research do not allow an individual to be identified.

7. Providing personal data to third parties

We need to treat the personal data that people entrust to us with all the confidentiality they expect. But there are many circumstances in which it is in their interests and ours to give information to third parties. The Fair Processing Notices for students (in the Student Handbook) and staff (on the HR website) set out the routine cases.

6.1 One-off inquiries

Usually, staff should not give out personal data to third parties (anyone other than the data subject and the University) unless there is a written agreement to do so. There are some circumstances in which one-off inquiries can be answered positively, but particular members of staff have been nominated to do so:

- Inquiries from the Home Office about international students are covered by a separate Procedure Note. They should be referred to the Home Office HE Compliance Co-ordinator.

- Inquiries about crime prevention or detection, typically from the police, benefit fraud investigators or insurance investigators. They should be referred to the Data Protection Officer.

- Inquiries from the courts. They should be referred to the Data Protection Officer (Dataprotection@sunderland.ac.uk) .

Otherwise, if in doubt, refer to the Data Protection Officer. In emergencies, if guidance is not available, refer to the questions about fairness in section 2.1, record your decision, the reasons for it, and the information disclosed, and pass on this record to the Data Protection Officer as soon as possible.

7.2 Freedom of information requests

In general, personal data should not be disclosed in response to a Freedom of Information request, but there are circumstances in which it might be ruled to be in the public interest to do so. Consult the Freedom of Information Officer for advice on sunfoi@sunderland.ac.uk .

7.3 Giving information to contractors

Sometimes, we will contract with organisations to perform tasks for us which require them to make use of personal data which we supply to them.

In these circumstances, the University remains legally responsible for everything the contractor does with that personal data. So the contract should contain clauses which set out the data we will transfer, the purposes for which it can be used, the standards we expect the contractor to adhere to, a right for the University to audit whether they are keeping to these standards, and an agreement for the contractor to reimburse the University for any costs we incur as a result of actions the contractor takes when handling personal data on our behalf. Contact Legal Services for how to do this, via the Data Protection Officer in the first instance.

7.4 Sharing information with partners

Sometimes, the University will agree to provide personal data to another organisation so that they can use that data for their own purposes. In some cases, that organisation may also be sharing data with the University for us to use for our own purposes.

In such cases, we should enter into a Data Sharing Agreement with the partner organisation, setting out the personal data involved, the purposes for which it is being transferred, and the terms and conditions on which it is being transferred. Contact Legal Services for how to do this, via the Data Protection Officer in the first instance.

8. Transferring data outside the EEA

Personal data can be transferred to another country in a variety of ways: by e-mail, letter or upload for example. It is counted as “transferred” even if it is only stored on a server in another country, despite being both uploaded from and only accessed by, UK-based users. Some Cloud storage providers will allow you to specify that your data will only be held on servers in one or more EEA countries, which would help to avoid problems.

All countries in the European Economic Area have similar data protection laws, giving effect to an EU Directive of 1995. The same rules therefore apply to transferring personal data to any of those countries as to transferring it within the UK.

The same rules also apply to transferring personal data to a few countries that the European Commission has certified as having adequate data protection: Andorra, Argentina, Canada, the Faroe Islands, Guernsey, the Isle of Man, Israel, Jersey, Switzerland and Uruguay.

Some organisations in the United States of America will have been certified as complying with the "Safe Harbor" scheme. The US government takes the view that such organisations have data protection in place that meets the EU's requirements. At the time of writing, the European Commission is considering whether or not it agrees. In the meantime, the University has to reach its own view about whether to regard Safe Harbor as sufficient protection, given the type of personal information being transferred, and what risks we believe exist. Contact the Data Protection Officer (Dataprotection@sunderland.ac.uk) for advice.

For transfers of personal data to any other country, our options are:

- Enter into a contract with the organisation or individual who receive the data which includes "model clauses" published by the European Commission, or clauses with an equivalent effect of binding the other party; or
- Undertake our own assessment of the adequacy of data protection law and practice in the other country, given the type of personal information being transferred, and what risks we believe exist.

In both cases, you will need to involve Legal Services. Contact the Data Protection Officer in the first instance.

9. Data breaches

Sometimes, despite everyone's best efforts, things will go wrong. If you think data has been misused – and particularly if it has been lost, published wrongly or given to someone who should not have it - please notify the Assurance Manager (Information Governance) and the Director of Business Assurance, who acts as the University's Senior Information Risk Officer (SIRO). They can both be reached on the e-mail address ba@sunderland.ac.uk .

It may sometimes be necessary to notify the Information Commissioner about a data breach. The SIRO will take that decision.

10. Staff's own personal data

Your own personal data, and its use by the University, is governed by the same rules as anybody else's. A Fair Processing Notice about how the University uses staff data is available from the Human Resources website.

If you have any queries about how your own personal data is being used, or want to exercise any of your rights under the Data Protection Act (see section 4 above), please contact the Data Protection Officer on Dataprotection@sunderland.ac.uk .

Appendix A: Useful Contacts
As at 5 December 2013

Data Protection Officer:
Steven Flanagan
Legal, Governance & Business Assurance
4th Floor
Edinburgh Building
City Campus
Sunderland SR1 3SD

0191 515 2508

Dataprotection@sunderland.ac.uk

Assurance Manager (Information Governance)
Maureen Wilkinson
Legal, Governance & Business Assurance
4th Floor
Edinburgh Building
City Campus
Sunderland SR1 3SD

0191 515 2485

ba@sunderland.ac.uk

IT Security Manager
Darren Ayre
IT Services
Unit 1 Tech Park
City Campus
Sunderland SR1 3SD

0191 515 2985

Senior Information Risk Officer
David Balme
Director of Business Assurance
Legal, Governance & Business Assurance
4th Floor
Edinburgh Building
City Campus
Sunderland SR1 3SD

0191 515 2407

ba@sunderland.ac.uk

A**ppendix B: Fair Processing Notice for Students**
Taken from the Student Handbook for 2013/14

The University Of Sunderland is registered as a data user with the Office of the Information Commissioner. Any personal data collected and or processed by the University is held in accordance with the provisions of the Data Protection Act 1988.

The University collects and holds personal data relating to its students for a variety of purposes. These include:-

- Facilitating the enrolment process;
- supplying operational services , including teaching and other forms of education;
- organisation of study abroad;
- organisation of work placements, internships, volunteering and student jobs;
- maintenance of the student record (including but not limited to personal and academic details) and management of academic processes (for example, academic audits, examination boards and awarding degrees);
- operating a biometric attendance register system;
- meeting the University's responsibilities under immigration law;
- management of student accommodation;
- general routine administrative functions such as access to buildings and library borrowing (which will include the use of an individual's photograph as it appears on their student card);
- publishing information (such as on examination notice boards, and for University prospectuses and marketing materials);
- use of photographs on the University website and in marketing materials either taken direct from the student card or taken specifically;
- operating a CCTV and automatic number plate recognition system;
- the provision of advice and support to students (via, amongst others, Student Services, Student Accommodation Services, the Advice Service, the University of Sunderland Students' Union, and the Careers Service);
- operating the Day Nursery (some nursery staff may be provided with limited access to some student information for the purposes of billing and administration); and
- alumni operations and correspondence which may be sent to you during your time at the University and continue to be sent to you after you have left the University.

The University (via academic departments, Student Services and other ancillary departments) discloses student information to a variety of recipients, including third party organisations, some not connected to the University including but not limited to:

- employees and agents of the University;
- the University of Sunderland Students' Union;
- students' sponsors, loans organisations and scholarships schemes (such as LEA's, the Student Loan Company, and funding councils);
- the Higher Education Statistics Agency (HESA) - further details can be obtained from www.hesa.ac.uk/collection-notices ;
- the Higher Education Funding Council for England (HEFCE) or their agents;
- relevant government departments or agents acting on their behalf to whom the University has a statutory obligation to release information (including, but not limited to, the Home Office, Council Tax Offices, Local Authorities, the Child Support Agency, the Benefits Agency, the Department of Work and Pensions);
- Higher Education Institutions (where exchange or placement programmes are being undertaken);

- employment agencies, prospective employers and third parties requesting confirmation of awards;
- current or potential employers of students;
- current or potential providers of education to students including, but not limited to, partner or franchise institutions in connection with the delivery of academic programmes of education; and
- the providers of the Campus Card.

The University may process sensitive personal data about you, such as details about your mental or physical health and/or disability, information concerning ethnicity, domicile, religious or political opinions, sexuality, criminal record, or alleged criminal activity for the purpose of planning or monitoring. In limited circumstances the University may also disclose this sensitive personal data to third parties, where there is a legitimate need or obligation, during or after your study.

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 – the University's Data Protection Officer should be contacted if students have any specific questions. Please note that the University is reliant on students for much of the data it holds: please help the University to keep records up to date by notifying any alterations to student addresses, personal details, or course enrolments.

The University may wish to contact you when you have completed your programme of study to inform you about products or services which may be relevant to you, and to keep you informed about University activities.

The University complies with the requirements of the Data Protection Act 1998. Guidance on Data Protection issues can be found in the Data Protection Policy and the Data Protection Guidance available on request from the Data Protection Officer.

Under the Data Protection Act 1998 an individual has the right to a copy of the current personal information held on them by the University and a right to raise an objection to data processing that causes unwarranted and substantial damage and distress. It should be noted that although you can object in some circumstances, the University may be required to hold certain information in order to deliver the course in question and to comply with specific sections of the Data Protection Act 1998. To discuss any objections or concerns, or to obtain a copy of the current personal information held about you, please contact the University's Data Protection Officer at the following address:

The Data Protection Officer
University of Sunderland
4th Floor
Edinburgh Building
Chester Road
Sunderland
SR1 3SD

Or send an email to: dataprotection@sunderland.ac.uk

Appendix C: Fair Processing Notice for Staff

As at 5 December 2013

The University is registered as a data controller with the Office of the Information Commissioner. Any personal data collected and or/ processed by the University is held in accordance with the provisions of the Data Protection Act 1998. The University collects and holds personal data relating to its staff for a variety of purposes. These include:

- the production of a University directory (which is available to the general public, online and in hard copy format);
- supplying operational services and external relations and development;
- production of University prospectuses and marketing literature promoting the University's activities, which may be sent overseas;
- the administration of a member of staff's employment relationship with the University;
- the production of returns required by government bodies;
- equal opportunities monitoring;
- providing staff with information on local and other events and facilities which may be of interest;
- general routine administrative functions such as access to buildings and library borrowing (which will include the use of an individual's photograph as it appears on their staff card);
- use of photographs on the University website and in marketing materials (taken for the University staff card);
- operating a CCTV and automatic number plate recognition system, in accordance with the University's published policies;
- operating the Day Nursery (some nursery staff may be provided with limited access to some staff information for the purposes of billing and administration);
- administrative procedures which may require the transfer of personal data about you to any organisation owned by or affiliated with the University; and
- any organisation (data processor) acting under contract to the University to process personal data which it holds.

The Data Protection Act defines some personal data as "sensitive", namely details about your mental or physical health and or disability, information concerning ethnicity, domicile, religious or political opinions, sexuality, criminal record, or alleged criminal activity for the purpose of vetting, legal compliance, planning or monitoring. The University may process some sensitive personal data about you. In limited circumstances the University may also disclose this sensitive personal data to third parties, where there is a legitimate need or obligation, during or after your period of employment.

Under the Data Protection Act 1998 an individual has the right to a copy of the current personal information held on them by the University and a right to raise an objection to data processing that

causes unwarranted and substantial damage and distress. It should be noted that although you can object, in some circumstances the University may be required to hold certain information in order to carry out its legitimate business and to comply with specific sections of the Data Protection Act. To discuss any objections or concerns, or to obtain a copy of the current personal information held about you, please contact the University's Data Protection Officer. You should send an email to dataprotection@sunderland.ac.uk or write to:

The Data Protection Officer
University of Sunderland
Legal, Governance and Business Assurance
4th Floor, Edinburgh Building
Chester Road
Sunderland SR1 3SD

The University complies with the requirements of the Data Protection Act 1998. Guidance on Data Protection issues can be found in the Data Protection Policy and Data Protection Guidance available from the Data Protection Officer on request.

Personal Information

Data Protection Act 1998

The University handles a lot of information about people – students, staff and others. Using that information effectively is an important part of our business, but we also have a responsibility to keep people's information safe, secure and confidential. Everyone who works for the University shares that responsibility.

If you have personal information about someone, you should

- Let that person see it if he or she asks
- Only use it, or show it to someone else, on the University's legitimate business
- Keep it safe from accidental disclosure
    - Mark it "Confidential" (or "Sensitive" if the information is sensitive)
    - Use passwords and encryption for electronic data
    - Keep paper files under lock and key.

If you keep information about an individual

- There must be enough of it for your purpose, but no more than that
- You must keep it accurate and up to date
- You must dispose of it securely when no longer needed.

If someone asks you for personal information

- Check that they are who they say they are
- Check that they've got a right to it
- Send it securely
- Don't send it outside the European Economic Area unless there's a proper contract in place.

If the person whose information you hold

- Asks you to stop making any use of it, you must consider that request
- Asks you to stop using their information for marketing, you must stop.

If you are working with an outside organisation

- Check whether any personal information will change hands and set out the terms in a "data sharing agreement".

Queries? dataprotection@sunderland.ac.uk