

A Confidentiality and Data Protection guide for staff

Contents

Introduction:

- What is confidential information?
- When might I come across confidential information at the Greenwich Students' Union (GSU)

The Data Protection Act 1998:

- Sensitive Personal Data

Disclosure of confidential information:

- Nature of the information
- When can I disclose sensitive and/or confidential information?

Duty of Care:

- Involving family or friends
- So what about a duty of care?
- Getting advice on confidential matters

Introduction

What is confidential information?

Confidential information is any information to which the common law 'duty of confidence' applies. A duty of confidence is created when 'private' information has been passed in such a way that the person receiving the information was aware of its confidential nature. The legal test is whether a 'reasonable person' would think the recipient ought to have known that information was confidential. A 'reasonable person' can be defined as a prudent person who normally exercises due care while avoiding extremes of both audacity and caution.

Read more: <http://www.businessdictionary.com/definition/reasonable-person.html>

Once you have obtained confidential information, you are under a common law obligation not to discuss or disclose it in any way, without the consent of the person who provided the information, except in very specific circumstances, set out below:

- If they believe students will cause serious harm to themselves or others.
- If you have cause for concern that a child/vulnerable adult may be suffering or likely to suffer significant physical, sexual or emotional abuse or neglect must inform the Social Services.
- We are obliged to share information subject to a Magistrates' Warrant. The authority may be in the form of a court order, warrant of control or writ of control.
- It is necessary to comply with our legal duties under Prevention of Terrorism legislation.
- We are concerned that there is a significant risk to your safety, or to the safety of other staff, students or other people unless we break confidentiality.
- You are incapable of giving consent to share information (for example, due to intoxication or mental ill-health) and it is necessary to break confidentiality to protect your welfare.

When might I come across confidential information at the Greenwich Students' Union?

- 1) All staff have access to the MSL online portal, which contains the personal data of all its members. You will use MSL for various functions and especially on Reception or the Activities Helpdesk but misuse of the software can not only lead to the SU's disciplinary procedure but can also lead to criminal or civil prosecution, as data is protected by The Data Protection Act (DPA) 1998, which is covered in more detail in the next section of this guide. If handling the information on MSL is part of your job description and therefore you cannot abuse your role and the information acquired whilst carrying out your day to day responsibilities. You should also be mindful that you are able to use the MSL portal in case of an emergency and we

need to find a member's next of kin, for example if the member is too drunk in a bar or is taken ill.

- 2) Employees at the SU are required to attend meetings with other members of the SU, External Trustees and other general associates. In these meetings the employee may be privy to personal/sensitive data. For example, if you attend any Trustee Board meetings or if the chair of the meeting specifically expresses that the content of the meeting is confidential. It is up to the employee to retain the information and understand that the information discussed should not be discussed outside of that meeting unless absolutely necessary, certain circumstances detailed below.
- 3) If your role means you come into contact with Human Resources files then you should understand that all the content is personal data and thus protected under the Data Protection Act (DPA). This includes: recruitment and selection, employment records, monitoring at work and Information about workers health. HR records and data must only be kept for as long as necessary for its purpose and then destroyed appropriately.
- 4) The employee should understand that all SU information they come into contact with during their time in employment, whether it is on the U Drive, via email or a conversation, is the property of the SU and should not leave the premises unless specifically agreed with their line manager. This includes via email, USB or any hard copies of files.
- 5) Employees may also witness an individual visiting the Advice service provided by the SU and in this case should also not disclose what they have seen with anyone unless the individual is happy to discuss this and reach this conclusion on their own.
- 6) There may be information held by our Commercial Services Department which is used on projects and commercial files that we won't want any competitors to come into contact with. This information must stay within the SU and can only be removed with the permission of your line manager.
- 7) Some data is allowed to be shared with others under certain circumstance such as a telephone/email enquiry which needs to be directed to another member of staff. In this case you can give out the staff email or contact number but no other details. You cannot pass on any information that is considered confidential, such as personal calls.

Information about the Data Protection Act 1998:

Sensitive (and or) Personal Data:

- Personal Data
- Sensitive Personal Information
- In Practise at the SU

Personal data means data which relates to an individual and includes any expression of opinion about that individual. This means personnel records, including sickness absence, performance appraisals, recruitment notes etc. will clearly be personal data. The DPA also gives extra protection to certain types of personal data called Sensitive Personal data which includes information about the subject's race, ethnicity, politics, religion, trade union status, health, sex life or criminal record (see below). Such data should be treated with particular care.

In addition, the Information Commissioner, and the Commissioner's office (ICO) who protect and enforce the DPA, considers that financial data, although not technically defined as 'Sensitive Personal data' under the DPA should be treated in the same way.

Personal Data (information taken from ICO website¹):

Information about individuals, that is kept by an organisation on computer in the employment context, will fall within the scope of the Data Protection Act and therefore, within the scope of this code. However, information that is kept in simple manual files will often fall outside the Act. Where information falls outside the Act, this code can do no more than offer advice on good information handling practice.

Personal information

The code is concerned with 'personal information'. That is, information which:

- is about a living person and affects that person's privacy (whether in his/her personal or family life, business or professional capacity) in the sense that the information has the person as its focus or is otherwise biographical in nature, and
- identifies a person, whether by itself, or together with other information in the organisation's possession or that is likely to come into its possession.

This means that automated and computerised personal information kept about workers by employers is covered by the Act. It also covers personal information put on paper or held in any 'relevant filing system'. In addition, information recorded with the intention that it will be put in a relevant filing system or held on computer is covered. Only a well-structured manual system will qualify as a relevant filing system. This means that the system must amount to more than a bundle of documents about each worker filed in date order.

¹ Data Protection – The Employment Practices Code https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

Processing

The Act applies to personal information that is subject to 'processing'. For the purposes of the Act, the term 'processing' applies to a comprehensive range of activities. It includes the initial obtaining of personal information, the retention and use of it, access and disclosure and final disposal.

Examples of personal information likely to be covered by the Act include:

- Details of a worker's salary and bank account held on an organisation's computer system
- An e-mail about an incident involving a named worker
- A supervisor's notebook containing information on a worker where there is an intention to put that information in that worker's computerised personnel file
- An individual worker's personnel file where the documents are filed in date order but there is an index to the documents at the front of the file
- An individual worker's personnel file where at least some of the documents are filed behind sub dividers with headings such as application details, leave record and performance reviews
- A set of leave cards where each worker has an individual card and the cards are kept in alphabetical order
- A set of completed application forms, filed in alphabetical order within a file of application forms for a particular vacancy.

Examples of information unlikely to be covered by the Act include:

- Information on the entire workforce's salary structure, given by grade, where individuals are not named and are not identifiable
- A report on the comparative success of different recruitment campaigns where no details regarding individuals are held
- A report on the results of "exit interviews" where all responses are anonymised and where the results are impossible to trace back to individuals
- A personnel file that contains information about a named worker but where the information is simply filed in date order with nothing to guide a searcher to where specific information, such as the worker's leave entitlement, can be found.

Sensitive personal information

What is sensitive data?

Sensitive data are information concerning an individual's;

- Racial or ethnic origin
- Political opinions
- Religious beliefs or other beliefs of a similar nature
- Trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- Physical or mental health or condition
- Sexual life
- Commission or alleged commission of any offence, or
- Proceedings for any offence committed or alleged to have been Committed, the disposal of such proceedings or the sentence of any court in such proceedings

Sensitive data processed by an employer might typically be about a worker's;

- Physical or mental health – as a part of sickness records revealed through monitoring e-mails sent by a worker to his or her manager or to an occupational health advisor
 - Obtained as part of a pre-employment medical questionnaire or examination.
 - Drug or alcohol test results
- Criminal convictions
 - To assess suitability for certain types of employment
- Disabilities
 - To facilitate adaptations in the workplace – to ensure special needs are catered for at an interview or selection testing – in monitoring equality of opportunity
- Racial origin
 - To ensure that recruitment processes do not discriminate against particular racial groups
 - To ensure equality of opportunity
- Trade union membership
 - To enable deduction of subscriptions from payroll
 - Revealed by internet access logs which show that a worker routinely accesses a particular trade union website.

In Practise at the SU

SU Property

If the SU has provided you with a work phone/tablet or laptop in order for you to effectively fulfil your role requirements, this equipment is not to be used for any personal actions. Any personal detail supplied via this method is property of the SU and they have the right to access this information if they need to.

If you decide that you would like to use your own phone/tablet or laptop to conduct your work there will need to be adequate security measures in place to avoid leaked information.

Disclosure of confidential information

Nature of the information

At some point you may be asked to keep something confidential that to you might not seem to be confidential or even important, however if you have been asked then it will contain some confidential relevance. Unless the information has already been made public by the subject of that information (no one else!), you should treat it as confidential and not disclose it inappropriately.

When can I disclose sensitive and/or confidential information?

Mentioned briefly above, there are circumstances when the information can be disclosed. Confidential information can be discussed with those who are already party to it, as long as this is within reason. It can also be disclosed when the subject of the confidential information agrees for it to be disclosed.

If the person does not agree to the disclosure, the information can still be disclosed under the below circumstances:

- When the vital interests of any person are threatened and the disclosure is made to a relevant and appropriate person;
- When it is in the public interest to do so and the disclosure is made to relevant and appropriate person.

Whenever an obligation of confidence is to be broken without consent, the other party should be informed, unless the grounds are the protection of the other party's vital interests and this would further endanger them.

Duty of Care – In practice at GSU

1. Greenwich Students' Union may put you on training courses, if they feel that it is necessary for you to take part. In such an event it is mandatory to attend.
2. It is not acceptable to share confidential information with the friends and/or family members of the subject of the confidentiality.
3. Duty of care can extend to directing those in need to the appropriate person and encouraging them to seek the support available. With the permission of the person you can refer a student to the Advice Services. For example, where the confidentiality refers to the person's disability and they have confided this information with yourself but they do not wish for anyone else to know, the possible limitations should be explained, as the SU may need to make reasonable adjustments.
4. When a matter arises that is not one of the above specified circumstances then you may wish to seek help and advice on how to appropriately move forward. You can do this without identifying the individual to which the matter relates, and you should seek guidance from the Advice Services or your line manager. You should not feel like you have to take on the burden yourself and you are encouraged to seek help from either of the aforementioned. Also, if someone approaches you and they feel confident enough to tell you they have a problem or an issue but you don't feel you are equipped to deal with it, then simply tell the person this and either pass the details of Advice or raise the concern you have for them again to either Advice or your line manager.