Staffordshire University Students' Union

Charter to the Data Protection Act 1998

Aims of the Data Protection Act

The Data Protection Act (DPA) compels Staffordshire University Students' Union to take specific measures to ensure that all personal information held about living (identified or identifiable) individuals in any file is processed according to eight Data Protection Principles.

The Act allows individuals to obtain a copy of their own personal data, the right to have inaccurate personal data corrected or erased and, where appropriate, to seek redress for any damage caused. In addition, the Act obliges Staffordshire University Students' Union to provide a complete description of all sources, to the Office of the Data Protection Registrar. The Act provides for criminal offences if these obligations are neglected. The Act also covers any personal data processed on Staffordshire University's Students' Union behalf e.g. by a payroll bureau.

The Students' Union should be aware of their responsibilities towards all personal data it holds. This is especially important in the case of all Staffordshire University Union - Students and Staff as we process personal data of a very sensitive nature.

Changes to the Law

In the Data Protection Act 1984 only files which were processed automatically e.g. by computer were covered by the Act. Under the Data Protection Act 1998 ALL personal data processed by Staffordshire University Students' Union is now covered. This means that, with effect from October 2001, manual files are covered as well as computer, video, microfilm, CCTV and any other medium. So assuming that because you never use a computer you do not need to bother about Data Protection means you could find yourself breaking the law.

The new Act is now targeted towards protecting an individual's privacy and so all processing of personal data must be justified. Personal data now includes any comments or opinions recorded about the individual as well. YOU are responsible for any processing of Personal Data that you perform in the line of your duty at the Union.

Aims of this Code of Practice

This guide is intended to aid Staffordshire University Students' Union staff to comply with the provisions of the Act. In particular, it is intended to:

(a) assist you to realise your obligations under the Act.

and

(b) indicate the practical steps to be taken to comply with the Act.

What is Personal Data

Personal data is information relating to a living person who can be identified:-

- from the data or,
- from the data and other information in the Union's possession or data likely to come into the possession of the Union.

For example a file with only a student's reference number is classed as personal data as this can be cross-referenced and the student identified.

Not only does personal data include personal identifiers such as name, address, reference numbers etc. It also includes any expression of opinion about the individual and any indication of the Union's intentions or the intentions of any other person in respect of that individual.

Personal data is described as "Sensitive" falls under much tighter controls. Sensitive personal data is data consisting of information as to their racial or ethnic origin, their political opinions, their religious beliefs or other beliefs of a similar nature. Whether they are a member of a trade union, their physical or mental health or condition, their sexual orientation and the commission or alleged commission by them of any offence or any proceedings for any offence committed or alleged to have been committed by them.

To process sensitive data the Union must have met several conditions for processing. This includes gaining explicit consent from the individual.

What is Processing?

"Processing" means obtaining, recording or holding any information in relation to personal data. It also includes carrying out any operations on that data as well as disclosing it. This means that every time you use any personal data you are "processing" it and therefore fall under the guidelines of the Act.

An Individual Rights

The act gives an individual certain rights, although some exemptions can apply. An individual has the right to make a "Subject Access Request". This allows them to see all information held by the Union about them with very few exceptions. This must be done in writing to General Manager of the Students' Union who is the Data Protection Officer of the Union. A fee of £10 is currently charged to cover any administrative costs.

Other rights include the right to:-

- prevent any direct marketing
- prevent processing in certain circumstances (e.g. automated decision taking such as psychometric tests)
- rectify, block, erase or destroy inaccurate data or to cease holding such data in a way incompatible with the Union's legitimate purpose.

Data Protection Principles

All processing of Personal Data must comply with eight Data Protection Principles. In brief these are as follows:-

1. Personal data shall be processed fairly and lawfully.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose shall not be kept for any longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of the individual under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage, to personal data.

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

Disclosing Personal Data

To other employees of the Union

Personal data may be disclosed to other employees of Union ONLY if they require the information to perform any duties in respect of their position within the Union. The release of personal data is NOT permitted merely for social reasons.

If you do not know the person requesting the information ask to see their identification badge. This not only proves who they are but also that they are employees of the Union. If the enquirers is on the phone arrange to call them back on a recognised University/Union number. If you are still unsure you can check with the Development Department or the Manager of their department who will be able to confirm their identity.
If in doubt, refer them to the Union's Data Protection Officer.

To prosecuting agencies such as the police

These enquiries should ALWAYS be referred to the General Manager or President unless they are not available AND the matter is urgent.

Urgent means – the individual is in danger or is a danger to others or has committed or is about to commit an offence.

If this is the case the police officers should issue you with a DP1 form (sometimes referred to as a section 29(3) form). On this form you will find:-

the identification of the person they are requesting the information about
the information they require
the reasons why they require the information
how the absence of any information would prejudice the enquiry.

This form must be signed by their Superintendent. Make a note of the Officers identification number. The form must be forwarded to General Manager immediately and marked confidential. Also include a list of the information actually released and the date and time this occurred as well as identifying yourself.

A Court Bailiff is not classed as urgent and must be referred to the General Manager or in their absence the Development Manager.

To the Media

All enquirers from the media should be referred to the President or the individual deputising in their absence. You must not even confirm whether the person is a student or employee of the Union.

E-Mail

The content of e-mails comes under the guidelines of the Data Protection Act. Any e-mail correspondence about an individual you send or receive will need to be archived and kept for as long as is appropriate for the content of it.

Staffordshire University Students' Union employees must ensure that you have a disclaimer on their e-mail content in line with the Students' Union E-mail best practice policy.

Shared Drives

If you have set up on your PC a shared drive / folder it is your responsibility to ensure that information security is not compromised. You have responsibility and liability if you process personal data. You must be particularly careful not to disclose personal data to anyone who does not have the right to access it. All staff who now require access to shared drives will need to complete a request for file storage shared area which is available on the Union Shared Drive in the NT / Shared Account Information file. It is the Line Managers responsibility to communicate the guidelines to their staff and approve access before forwarding this information to Administration Assistant at Stafford.

Confidentiality

The Students' Union understands confidentiality to mean that no information regarding a service user shall be given directly or indirectly to any third party external to the Students' Union, without the service user's prior consent to disclose such information.

It is the responsibility of the staff member and Development Department to ensure that where an individual requires someone to act on behalf of them that a Form of Authority is completed. The original is to be kept on file and a copy enclosed when corresponding with any third parties.

To relatives, friends, landlords or other related enquirers not covered in previous section

You cannot disclose information to the above category of people. If they do contact you offer to transfer them to the General Manager or Development Department if they are enquiring about a student or personnel about a member of staff. When doing this avoid disclosing any information about the individual. This even includes whether or not they work, volunteer or study at the Union / University.

If the caller is insistent or "difficult", you should ask whether it is possible for the caller to be phoned back at a later stage and refer the call to your line manager. Staff should try to be patient and calm.

The enquirer must be informed that
"Staffordshire University Students' Union respects the confidentiality of all personal information it hold under the Data Protection Act 1998 and as a result of this, information cannot be disclosed to them".

If the matter is urgent you can offer to pass on a message but again you must be careful that you do not disclose any information to them.

Do not be bullied into releasing information.

Forwarding Letters

In some circumstances, staff may be requested to forward letters on behalf of the enquirer, but they should make it clear they can give not guarantee of locating the person in question. Only if a letter actually arrived for forwarding should staff take time to try to trace the addressee and send on the letter. If in doubt, refer this to the Data Protection Officer.

Staff should ask the enquirer to enclose the letter in a sealed envelope, and to provide a stamped envelope endorsed with the name of the recipient, together with a formal written request for the letter to be forwarded.

This request should contain the last known whereabouts of the recipient and should be marked for the attention of the section or department who will deal with the request.

Staff should ensure that the letter to be forwarded is accompanied by a compliment slip explaining this action, and stressing that the recipient's address has not been disclosed to the sender of the letter.

Research

Personal data processed ONLY for research, historical or statistical purposes does receive certain exemptions as long as the following conditions are met:-

- it is exclusively used for this purpose
- it is not processed to support measures or decisions relating to a particular individual
- it is not processed in such a way that substantial damage or distress is likely to be caused
- the information will not be considered incompatible with the purpose it was obtained for.

Personal data recorded for this purpose may be kept indefinitely despite the Fifth Data Protection Principle.

The individual does not have the right to access this data provided that the results of the research or any resulting statistics are not made available in a form, which identifies them.

The data may be disclosed by the researcher only:-
- to any person for research purposes only
- to the individual themselves
- with the consent of the individual

Direct Marketing

Direct marketing is defined in the Act as the communication (by whatever means) of any Union advertising or marketing material, which is directed to particular individuals. This does not include marketing materials for companies or selling lists of names held by the Union on to other companies. If you wish to do this please contact the Union's Data Protection Officer for advice.

An individual is entitled to write to the Union to request that we cease or do not begin processing personal data relating to them for the purposes of direct marketing.

If as part of your role within Staffordshire University Students' Union and you use Direct Marketing you must ensure that when you obtain the details of an individual they are fully aware that this is what you will be using their information for.

A permanent record of those wishing to opt out from receiving any mailings must be kept. Information on your mailing list must be up to date and correct. A good practice procedure recommended by the Data Protection Commission is to give all individuals an opportunity to opt out from your mailing list once a year and check their details are still correct.

Opt Out

This is required on any information that we are collating on individuals. A box allowing an individual to opt out of any other information being sent to them from the Students' Union or on behalf of the Students' Union. The interpretation by law being that anything not opted-out of constitutes opted-in.

It is therefore essential that individuals are given the choice, all documentation requiring consent will need to have the Unions standard inclusion as follows placed on documentation, this will include such areas as; SMS messaging, client data, student data (loyalty schemes), volunteer consent, driver contact details, pre-booked ticket sales etc.

The Students' Union will use the information on this form to contact your regarding EG LRV Platinum (the purpose of business is inserted here). The Students Union may also wish to send you information from third parties about discounts, products and services, which may be of interest. Please tick ☐ this box if you would prefer not to receive such information.

Security of Personal Data

It is extremely important to make sure that all personal data you are responsible for is kept secure. If you do not and personal data is lost or falls into the wrong hands then YOU are responsible. You will have breached the Seventh Data Protection Principle and will therefore have committed an offence.

Simple Steps to Follow are:-

- Do not leave your office unlocked when empty.

- Make sure files containing personal data are not left lying around your office or desk but are filed away.

- Follow the guidelines for disclosing personal data.

- Ensure that communications distributed either internally or externally are secure. For example sealed envelopes or packages.

- Select a secure password for your computer account. This can be done by:-

♦ the use of a combination of alphabetic and no-alphabetic characters;
♦ avoiding use of real names or words, particularly ones that may be closely associated with you and know to others e.g. the name of your dog, cat, child etc.
♦ avoiding use of sequences of numbers or letters.

Your password must NOT be disclosed to anybody (including Union managers). You must take all reasonable precautions to ensure that your password remains confidential (don't leave it stuck to your computer on a post it note!!!!).

When you leave your PC unattended either log out or have a password protected screen saver set.

You must ensure that when disposing of personal data it cannot fall into the wrong hands. For example shredding files or destroying floppy disks could ensure that this does not happen.

References

The following advice applies to those providing references (internal and external) for present and past employees and students and to those receiving references.

Legal Position

- A reference can be the subject of an action for negligence as well as for defamation.
- The provider of a reference has a duty of care in the preparation of a reference. Thus employees can sue employers for damages for failure to exercise reasonable care.
- Recent case law has established that, where there is negligence, an employee does not have to prove actual loss of an appointment but only that she has lost a reasonable chance of employment and thereby sustained loss.
- It may also be that a duty of care is owed to the receipt of the reference, therefore the latter might be in a position to sue for negligence.
- The Data Protection Act 1998 applies to references.

1. Duty to Provide a Reference

Given the above, it might seem safer to opt out of providing references. However, there is an implied duty to provide a reference (as well as moral obligation) upon Managers toward staff, student staff or volunteers, whose careers they are in a position to influence.
Departmental policy on references should be made clear and agreed with the Development Department i.e. can they assume that they will automatically be provided with a reference or should you be approached first.

If you are asked to give an unsolicited reference (for a person who has not, to your knowledge, cited your name as referee), it is advisable to limit your information to the facts.

If you receive a request from a potential employer but are unable or unwilling to give a reference, then please discuss this with the Development Manager whom will support you in communicating your refusal.

2. Confidentiality

All references are given in confidence, but in some circumstances, they may be an obligation to disclose:

- If a copy is requested by the subject if the reference (DPA)
- If required by a Court or enforcement order
- Or if required in defending a claim for damages

3. The Data Protection Act

The Act states that a confidential reference, for the purposes of education, training and employment is exempt from subject access.

- Giving references - you may mark a reference 'confidential' in order to prevent you having to disclose it to the subject.
- Receiving references - if you receive a reference, whether or not it is marked 'confidential' you may be obliged to discuss its contents. However, the Act implies that you may legitimately refuse to disclose a reference if the refer does not consent to this it is not possible to keep the referee's identify confidential - the identity of the referee is also personal data - by blanking out names etc.

4. Telephone or Verbal References / Communication

These should also be handled with a similar degree of care, steps taken to confirm the identity of the person requesting the reference. If notes are kept of the conversation, these may be required to be disclosed. You should state that the reference is given 'without legal responsibility' and you reserve the right not to answer certain questions.

There are two principal aims of a reference:-

- To confirm facts
- To provide opinions as to the candidates suitability

The two should be clearly differentiated and you should try not to confuse fact and opinion.

5. Disclaimer

All reference should contain the following disclaimer:

'The Union accepts no liability, in negligence or otherwise, for the statements or information contained in this reference although they are given in good faith'.

There is no guarantee, however, that a disclaimer will not be challenged in court, therefore due care must be exercised in preparing a reference.
You are challenged over a reference you have given, do NOT admit liability. Consult the General Manager or Development Manager.

CCTV

The Data Protection Act has superseded the 1984 Act and now covers a number of other data storage and retrieval systems. There are now statutory regulations, which covers the use and management of CCTV systems, which record output.

Any member of the public or staff of an organisation, who have a justifiable reason, have the right to request access to any CCTV data that they believe a CCTV 'owner' holds, and which they appear. The current Act applies to all systems irrespective of size or purpose of use.

The Students' Union must therefore take all steps to ensure that the data recorded by the company is within the terms of the Act and in accordance with the principles laid down by legislation. The Students' Union have developed an organisational standard with should be held centrally within any department operating CCTV systems.

Summary

The New Data Protection Act 1998 imposes stringent requirements that any organisation holding personal data must comply with.

Everyone should be aware of the Data Protection Act, and their responsibilities, especially that individual staff members can be personally liable (a fine and criminal record) for breaches of the Act, if acting outside their authority.

The legislation states that all processing undertaken must be fair and lawful, accurate and up-to-date, and that the data is adequate, relevant, not excessive and is held for no longer than is necessary. It also becomes mandatory that appropriate technical measures are taken to prevent unauthorised or unlawful processing or disclosure of data. This includes accidental loss or destruction of, or damage to, personal data.

Personal data can only be processed if one of the following applies:

- an individual has given consent;
- that it is part of a contract;
- it is a legal obligation;
- it is necessary to protect the individual.

The rules also introduce “sensitive personal data”, which include any that are racial or ethnic in origin, political affiliations, religious or other beliefs. This data demands greater protection and one of the following must be true:

- an individual’s explicit consent is required;
- is a legal requirement
- to protect the VITAL interest of the individual.

Where consent is obtained, the individual must be made fully aware of the purposes for which the data is to be used and of any recipients.

Another change makes data held in manual or paper form subject to the Act. So any personal details stored in a paper format must be registered come under the guidelines of the Data Protection Act.

Individuals’ rights are extended with further provisions to enable them to see a full description of their personal data, on payment of a fee. This information has to be corrected if it is inaccurate or likely to cause damage or distress. Individuals can also request details of how automatic decision-making processes operate. There are also impacts on the use of data for direct marketing, either my mail or telephone. An individual can claim compensation for any damage or distress caused by breach of the Act.

Further Information

Further advice or guidance can be obtained from the University’s Data Protection Officer, Mr Ken Sankson, General Manager, extension 4377, e-mail: k.sankson@staffs.ac.uk.