Staffordshire University
Data Protection Policy

Introduction

Staffordshire University needs to gather and use certain information about individuals.

These can include customers, suppliers, business contacts, employees and other people the organisation has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the University's data protection standards — and to comply with the law under the Data Protection Act 1998.

This data protection policy ensures Staffordshire University

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Why this policy exists

This data protection policy ensures Staffordshire University

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection law

The Data Protection Act 1998 describes how organisations — including Staffordshire University must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

People, risks and responsibilities

Policy scope

This policy applies to all staff and all contractors, suppliers and other people working on behalf of Staffordshire University.

It applies to all data that the University holds relating to identifiable individuals, even if that information technically falls outside of the Data Protection Act 1998. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect Staffordshire University from data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the University uses data relating to them.
- **Reputational damage.** For instance, the University could suffer if hackers successfully gained access to sensitive data or sensitive data is lost.

Responsibilities

Everyone who works for or with Staffordshire University has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

- The only people able to access data covered by this policy should be those who **need it for their work**.
- Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.
- **Staffordshire University will provide training** to all employees to help them understand their responsibilities when handling data.

- Everyone processing personal information understands that they are **contractually responsible** for following good data protection practice.

- Everyone processing personal information is **appropriately supervised**.

- Anybody wanting to make enquiries about handling personal information **knows what to do**.

- Everyone deals **promptly and courteously** with any enquiries about handling personal information.

- Staffordshire University will regularly **review and audit** the ways it holds, manages and uses personal information.

- All staff are aware that **a breach of the rules** and procedures identified in this policy may lead to **disciplinary action** being taken against them

- Employees should keep all data secure, by taking **sensible precautions** and **following the guidelines** below.

    - In particular, **strong passwords must be used** and they should never be shared.

    - Personal data **should not be disclosed** to unauthorised people, either within the University or externally.

    - Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

    - Employees **should request help** from their line manager, departmental coordinator or member of staff with cross University responsibility (usually the Data Controller) if they are unsure about any aspect of data protection.

Data storage

These rules describe how and where data should be safely stored.

When data is **stored on paper,** it should be kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorised people could see them**, like on a printer.
- **Personal or confidential data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing service**.
- Personal data should **never be saved directly** to laptops, USB drives (unless encrypted) or other mobile devices like tablets or smart phones.

Data use

Personal data is of no value to Staffordshire University unless it can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**.
- Personal data must be **encrypted before being transferred electronically outside of the University**. The member of staff with cross University responsibility (usually the Data Controller) can explain how to send data to authorised external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

The law requires Staffordshire University to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort Staffordshire University should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject access requests

All individuals who are the subject of personal data held by Staffordshire University are entitled to:

- Ask **what information** the University holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the University is **meeting its data protection obligations**.

If an individual contacts the University requesting this information, this is called a subject access request.

Information about subject access requests is available from the University website http://www.staffs.ac.uk/legal/request_information/

Disclosing data for other reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, Staffordshire University will disclose requested data where the request is legitimate.

In addition **Staffordshire University** will ensure that:

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998.

In case of any queries or questions in relation to this policy please contact the Data Controller: foi@staffs.ac.uk .

Further information can be found on the University Legal Website:

- Data Protection: 10 rules for compliance
  http://www.staffs.ac.uk/legal/privacy/10_rules/index.jsp
- Data Protection: Frequently Asked Questions
  http://www.staffs.ac.uk/legal/privacy/data_protection_faq/index.jsp
- IT Policies and Regulations
  http://www.staffs.ac.uk/support_depts/infoservices/rules_and_regulations/index.jsp

Signed:

Position:

Date: June 2015

Review Date: June 2016