Information Security Management System (ISMS)

DATA PROTECTION POLICY

Document Hierarchy: Tier 1 Policy

Document Status: Final

Document Ref: DOC 15.6

Originator: S Pandya

Updated: D Bolton

Owner: Director – Technology & Corporate Programmes

Version: 03.02.01

Date: 01/12/15

Approved by Corporate Management Team

Document Location

This document is held by Tamworth Borough Council, and the document owner is Nicki Burton, Director – Technology & Corporate Programmes

Printed documents may be obsolete, an electronic copy will be available on Tamworth Borough Councils Intranet. Please check for current version before using.

Revision History

Revision Date	Version Control	Summary of changes
01/12/15	03.02.01	Amendment following departure of Corporate Information Security Manager
07/10/15	03.01.01	Add sections 10 and 11 and minor changes to policy throughout.
26/02/13	02.02.01	Scheduled review no change
15/11/10	02.02.01	Scheduled review no change
11/11/09	02.02.01	Document formatted to approved ISMS Standard and job titles changed.
11/06/07	02.01.02	Final document approved by Corporate Management Team.
02/02/07	02.01.01	Complete review of existing document
17/06/05	01.01.01	Document creation

Approvals

Name	Title	Approved
CMT	Corporate Management Team	11/06/07
CMT	Corporate Management Team	Dec 2015

Document Review Plans

This document is subject to a scheduled annual review. Updates shall be made in accordance with business requirements and changes and will be with agreement with the document owner.

Distribution

The document will be available on both the Intranet and the approved Tamworth Borough Council Website.

Security Classification

This document is classified as OFFICIAL, accessible to all.

CONTENTS PAGE

1 PURPOSE OF THE DATA PROTECTION POLICY

1.1 SCOPE

Tamworth Borough Council obligation is to ensure compliance with the Data Protection Act 1998. The Information Commissioner who oversees compliance and promotes good practice requires all data controllers who process personal information to be responsible for their processing activities and comply with the eight data protection principles of 'good information handling'.

These are:

Principle 1:	**Personal data shall be processed fairly and lawfully.**
Principle 2:	**Personal data shall be obtained for one or more specified and lawful purposes.**
Principle 3:	**Personal data shall be adequate, relevant and not excessive.**
Principle 4:	**Personal data shall be accurate and, where necessary kept up to date.**
Principle 5:	**Personal data shall not be kept for longer than is necessary.**
Principle 6:	**Personal data shall be processed in accordance with the rights of data subjects.**
Principle 7:	**Technical and organisational measures shall be in place to keep personal data secure.**
Principle 8:	**No transfer outside of the EEA without adequate level of protection.**

This policy applies to all personal data held by Tamworth Borough Council and covers all formats, examples are; electronic, paper, magnetic, digital and video. This will also extend to all future formats that will be capable of recording, holding and storing personal information.

This Policy applies to all employees, elected members, temporary / contract staff that are directly employed, engaged or represent the council.

2 OVERVIEW OF THE DATA PROTECTION ACT

The Data Protection Act 1998 came into force 1st March 2000 with full implementation on 24th October 2001, and sets out rules for processing personal data recorded on all formats. This revokes the Data Protection Act 1984. The Act is a mandatory requirement for compliance for any organisation that collects personal information.

The 1998 Act enhances an individual's right to processing and access to personal information held by an organisation that in certain circumstances the data subject may have the information held by organisations corrected or erased, or they are able to prevent processing.

If by not complying with the Act causes harm and/or distress to the data subject, the council who will be referred to as the data controller could be prosecuted for serious offences, and the individual could also claim for compensation.

3 ORGANISATIONAL RESPONSIBILITIES

The Council will adhere to the **Data Protection Principles** and promote good practice in respect of obtaining, using and holding **personal data**. All use of personal data will be **notified to the Information Commissioner**.

In particular the Council will only disclose personal data in-line with its statutory responsibilities to undertake it functions / services for employees and service users. No voluntary release of data will be undertaken beyond the normal business requirements. In exceptional emergency circumstances data will be released where it is deemed appropriate.

The Council from time to time will be involved in specific work to protect public monies from fraud and the prevention or detection of crime. The Council will advise **data subjects** at the time of obtaining their information that this data may be used in connection with this type of activity.

The Council will hold minimum personal data necessary to enable it to perform its functions. Every effort will be made to ensure that information is accurate and up to date and that inaccuracies are corrected without unnecessary delay. Only matters of fact will be recorded and which can be substantiated at a latter date. Any opinions expressed will be based on reliable information and in a professional manner.

The Council will retain personal data only far as long as is absolutely necessary in order to comply with legal, statutory or legitimate business function purposes. It will be the responsibility of each Director or Head of Service to inform the Director – Technology & Corporate Programmes of this **retention period** for each class of data under their control and to arrange, in conjunction with Information Services, secure destruction of expired data.

The Council will respond to and **assist every request for access to personal data** from those subject to the personal data processed about them. The Council may charge for access to personal data as permitted by the Act's provisions. It will be the duty of the Director – technology & Corporate Programmes or nominated Deputy to ensure the Council meets it legal obligations.

The Council will ensure any Member / Officer who has access to the Council's personal data at non-Authority sites will be authorised, and made aware of their responsibilities, for the safe custody of that data whilst in their possession.

Personal data will be kept in an appropriately controlled and secure environment. The Council will seek to adhere with the provisions of the security standard ISO27001 promoted by the Information Commissioner, although will not secure certification against this standard

Data Sharing / use with external organisations will be the subject of a written agreement covering the scope of data to be used, controls to protect personal data and where necessary the reasons permitting the sharing / use of the data.

The Council will ensure all employees, elected Members and temporary / contract staff receives appropriate training / guidance regarding their individual responsibilities under the Act's provisions.

Any member of staff knowingly or recklessly breaching the Council's Data Protection Policy will be subject to the **internal disciplinary procedure**. Matters relating to Elected Member non-compliance will be reported the Standards Committee for review.

4 CONFIDENTIALITY AND SECURITY

Personal data will be classed as confidential and treated as such. Appropriate security shall be in place to prevent loss, unauthorised changes or unauthorised disclosure in accordance with the provisions of the Act.

It is the duty of every person who is granted authorised access to this personal information to ensure that this asset is not knowingly or recklessly misused.

- **Manual Files**: Access must be restricted solely to relevant staff and stored in secure locations to prevent unauthorised access.
- **Computer Systems** Will be configured with appropriate security levels to preserve confidentiality. Users will only have access to personal information that is necessary for the purposes of carrying out their function.
- **Information Security** Users must comply with the councils information security policies, guidelines and procedures.
- **Disclosures** Personal data shall only be disclosed to the data subject and other organisations and persons who are notified recipients within the councils notification register held at the Information Commissioners office. There may be occasions where personal data is requested to be disclosed either under one of the exemptions contained within the Act, or under other relevant legislation. There is a requirement to keep an audit trail to provide accurate details of this disclosure.
- **Sensitive Personal Information** Additional obligations are placed on the council under the **first principle** that after meeting one or more of the conditions in schedule 2 at least one of the conditions must be met in schedule 3 of the Act. Schedule 3 conditions are that either the data subject has given their **explicit** consent or that the processing is **necessary** for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the council.

5 OWNERSHIP OF DATA

Each department is responsible for the personal data it holds. The responsibility also extends to personal data that is processed by a third party on behalf of Tamworth Borough Council. The departments will hold a record of all its processing activities containing personal

information, irrespective of format. Where required each department will provide the necessary information to the Director – Technology & Corporate Programmes in order to facilitate the notification of the dataset with the Information Commissioner.

Internal notification to the Director – Technology & Corporate Programmes of creation, deletion or changes in datasets is a process in which the council keeps a check of its processing activities. The Director – Technology & Corporate Programmes has the responsibility to ensure the council's notification register with the Information Commissioner is accurate and up to date; **failure to do this is a criminal offence.**

6 PROCESSING INFORMATION

'Processing', in relation to personal data, means obtaining, recording, using or disclosing that data.

This includes organising, adapting, amending and processing the data, retrieval, consultation, erasure or destruction.

All processing of personal data will comply with the provisions of the Data Protection Act 1998. In the situation where a third party processes the data, the third party will be required to act in a manner which ensures compliance with the Act, and have in place adequate safeguards to protect that data.

6.1 OBTAINING

Any data collection forms used in order to record personal information will contain a 'fair processing' statement. This should be clearly visible and placed appropriately on the form detailing our duties under the Act. The statement should also contain the following information:

- The identity of the data controller, contact for submitting subject access requests.
- The purpose or purposes for which the information is intended to be processed.
- Any foreseeable third parties that the information is intended to be disclosed to.
- Any further information in order to make the processing fair.

When collecting information over the telephone, or face to face the above information should also be made clear to the data subject **before** any processing of their personal data takes place.

6.2 RECORDING AND USING THE DATA

Data should only be used for the purposes it was collected, and should not be used for any additional purposes without the consent of the data subject.

Tamworth Borough Council has a duty to inform all individuals of why their personal data is being collected. Principle one of the Act stipulates that all personal data collected should be **fair and lawful** and processed in line with the purpose it was given. The Council may need to hold and process the information in order to carry out its statutory obligations, where this process takes place it will also be processed fairly and lawfully.

6.3 DISCLOSURE

Person data must not be disclosed except to **authorised users**, other organisations and people who are pre-defined as a **notified recipient**, or if required under one of the **exemptions** contained within the Act.

7 DATA SUBJECTS RIGHTS

7.1 THE RIGHT OF SUBJECT ACCESS

Sections 7 to 9 of the Act gives a right for an individual to request access to their personal information upon written application to the data controller for information which they believe may be held by them.

If the Council does hold the requested information, then subject to any exemptions, will provide a legible copy to the applicant or their authorised recipient within 40 calendar days (prescribed period) of receipt of the subject access request. Alternatively the applicant or their authorised recipient may wish to view only the files. The files will be prepared in such a way to comply with the Act and arrangements made to allow privacy whilst inspecting, an appropriate officer must be in attendance at all times whilst this process is being carried out to maintain security of the documentation, this again must be carried out within the prescribed period.

The Council will be diligent in providing the information within the prescribed period, where this period is insufficient then the applicant must be informed, at the earliest possible time giving good reasons for the delay (resource shortage would not be considered a good reason). Where the period will be exceeded it is good practice to disclose any available information immediately and not wait until the package is complete.

If the applicant subject believes that Tamworth Borough Council has not responded correctly and are dissatisfied with the Council's response, they are entitled to lodge a compliant with the Information Commissioners office, who may carry out an investigation.

7.2 PREVENTION OF PROCESSING CAUSING DAMAGE OR DISTRESS

Section 10 of the Act entitles an individual to give notice in writing to the Council where they believe the processing of personal data causes them substantial unwarranted damage, or substantial unwarranted distress. This notice will request the data controller, within a reasonable amount of time, stop processing the data.

7.3 RIGHT TO PREVENT PROCESSING FOR PURPOSES OF DIRECT MARKETING

Section 11 of the Act entitles an individual to submit in writing to the Council requesting they cease, or not to begin, processing their personal data for direct marketing purposes. When this notice is received the Council must comply with the request as soon as practically possible.

If the Council does not comply with this request, the individual is entitled to apply to a Court for an order to cease this activity.

7.4 RIGHTS IN RELATION TO AUTOMATED DECISION TAKING

Section 12 of the Act entitles an individual, by written notice, to require the Council to ensure that no decision, which significantly affects that individual, is solely based on the processing by automatic means of personal data of which that individual is the data subject.

7.5 RIGHT TO COMPENSATION

Section 13 of the Act determines that an individual who suffers damage, or damage and distress, as a result of any breach of the Act by the Council, is entitled to lodge a claim for compensation where the Council is unable to prove that they had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

7.6 DEALING WITH INACCURACY

Section 14 entitles the data subject to apply to the Court for an order requiring the Council to rectify, block, erase or destroy such data relating to the data subject that is deemed inaccurate, together with any other personal data relating to the data subject which contains an expression of opinion which the Court finds is based on the inaccurate data.

8 TRAINING

All employees of Tamworth Borough Council that hold, have access to, or process personal information will receive appropriate training to comply with the Act.

Data Protection awareness is essential for all personnel that carry out these functions, and the Council will provide this awareness through a variety of methods, to ensure that compliance with the 8 data protection principles are known and understood and how they relate to their duties.

It is the responsibility of all managers to ensure that the appropriate level of training has been received by their staff.

9 SECURITY

Principle 7 of the Act states that the Council will have in place appropriate technical and organisational security to protect any personal and sensitive information that we process.

Additional to this is Tamworth Borough Councils commitment to British Standards ISO27001 Information Security, although will not secure certification against the standard, which is defined as:

"The protection of information from a wide range of threats in order to ensure business continuity, minimise business risk, and maximise return on investments and business opportunities"

Furthermore;

"Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives are met."

There are three key points that staff need to understand regarding information security:

- Information exists in many forms;
- Is a combination of management and technological process;
- We all have a role to play in keeping information secure.

10 CLEAR SCREEN CLEAR DESK

All staff, contractors and partners will operate a clear screen, clear desk policy. This requires everyone that has access to information considered to be personal as defined by the Act, to handle it with an appropriate level of security and confidentiality to prevent disclosure, accidental or otherwise to those not entitled to access it.

This places an obligation on those to ensure information is secured in approved receptacles such as lockable cabinets when not required and not left on desks or in trays unless the office itself has restricted access that prevents those accessing the information.

Computers shall be locked down when not in attendance with the approved screen savers on display or system turned off. The screens shall be positioned or shielded in such a way to prevent viewing by unauthorised persons.

This policy shall apply to the office and any remote working place.

11 BREACH REPORTING AND INVESTIGATION

The Council operates an internal Breach Reporting Procedure (BRP) where there is a claim or evidence of personal information being handled incorrectly. This BRP is used where:

- An internal report of a potential data breach is relayed to a manager or the Director – Technology and Corporate Programmes.
- An external report of a potential data breach is received in writing either directly to a member of staff, or through our customer facing services.
- Correspondence from the Information Commissioners Office (ICO) in response to a complaint against the Council

In the first instance the Director – Technology and Corporate Programmes (D-T&CP) shall receive the details of the potential data breach. If there is a conflict of interest then the case shall be handled by another officer with the appropriate seniority to investigate.

The D-T&CP can express discretion on a case by case basis to delegate part or all of the recording and investigation process.

Data breaches can be categorised as:

Major Data Breach - This is where the breach is considered to have a significant effect on the reputation of the Council, including it's partners. This includes actions whether be accidental or deliberate by staff contracted or casual, third parties and suppliers under contract to deliver the councils services and partners working alongside the Council.

The Chief Executive will need to be informed of the major data breach to consider proactive action to report the breach to the ICO, in accordance with the non statutory guidance https://ico.org.uk/for-organisations/report-a-breach/

Minor Data Breach - This is where the breach is not considered to have a significant effect on the reputation of the Council, including its partners. This includes some defective processes and accidental loss by staff contracted or casual, third parties and suppliers under contract to deliver the council's services and partners working alongside the Council

12 RELATED LEGISLATION

The following legislation is associated with the Data Protection Act 1998:

The Freedom of Information Act 2000
The Children's Act 1989
The Disability Discrimination Act 2005
The Human Rights Act 1988
The Environmental Information Regulations 2004
The Copyright, Patents and Designs Act 1988
The Computer Misuse Act 1990
The Defamation Act 1996
The Electronic Communications Act 2000
The Privacy and Electronic Communications Regulations 2003
The Regulation of Investigatory Powers Act 2000
The Re-Use of Public Sector Information Regulations 2015
The Civil Contingencies Act 2004
The Protection of Freedoms Act 2012
The Local Government Transparency Code 2014

13 GLOSSARY

Data controller A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Data processor	A person, who processes personal information on a data controller's behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.
Data subject	This is the living individual who is the subject of the personal information.
Notification	Notification is the process by which a data controller's processing details are added to a register. Under the Data Protection Act every data controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply with the data protection principles. The Commissioner maintains a public register of data controllers available at www.ico.gov.uk. A register entry only shows what a data controller has told the Commissioner about the type of data being processed. It does not name the people about whom information is held.
Personal data	Personal data means information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession.
Processing	Processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data.
Subject access request	Under the Data Protection Act, individuals can ask to see the information about themselves that is held on computer and in some paper records. If an individual wants to exercise this subject access right, they should write to the person or organisation that they believe is processing the data.

End of Document