INFORMATION SECURITY POLICY

Document Status: Final

Document Ref: InfoSecPolicy

Originator: Director of Technology & Corporate Programmes

Updated:

Owner: Director of Technology & Corporate Programmes

Version: 01.03

Date: 10/04/2018

Approved by GDPR Working Group

Classification: OFFICIAL

Document Location

This document is held by Information Services of Tamworth Borough Council, and the document owner is Director of 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
10/04/2018	1.02.00	Draft for comment
16/05/2018	1.03.00	Inclusion of feedback through consultation

Next Revision

Review Type	Date
Full Review	May 2019

Approvals

Name	Title	Approved
Andrew Barratt Anica Goodwin John Wheatley Nicki Burton Rob Barnes Jane Hackett Stefan Garner	Corporate Management Team	16/05/2018
	Trade Union Liaison Group	
	Cabinet	
	Full Council	

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 the Intranet and through NetConsent and accessed by authorised users.

Security Classification

This document is classified as OFFICIAL with access restricted to Tamworth Borough Council Staff and business partners.

Contents

1 Introduction

Information is one of the most important assets managed by Tamworth Borough Council. In recognising the value of our information assets, we also recognise that those assets must be used and secured in an appropriate way.

We are committed to preserving the confidentiality, integrity and availability of all of our information assets to enable ;

- Sound and effective decision making ;
- Our customers to maintain confidence in us as an organisation ;
- Compliance with legislation ;
- The maintenance of our reputation as a professional organisation ;
- Continued delivery of quality services to our customers.

This Policy outlines Tamworth Borough Council's approach to information security and is delivered in three parts ;

- Information Processing
- Information Sharing
- Controls

The Policy applies to all employees and Elected Members of the organisation, both permanent and temporary. It also applies to contractors, partners and visitors who are engaged to work with, or have access to, council information.

The Policy applies to all locations from which council systems and information are accessed, including home use. Where access is in place to enable external organisations to access council information, officers must confirm that their security policies meet the standards of this Policy. Copies of any third party policies should be obtained and retained with the relevant contract or agreement.

Third party processing agreements must be in place before enabling any third party access to information assets for which the council is responsible.

2 Policy Compliance

This Policy will be disseminated via NetConsent and is available on the council's Intranet

If any user is found to have breached this Policy, they will be subject to the organisation's Conduct and Capability Process. The policy can be found http://infozone.tamworth.gov.uk:901/sites/default/files/HR_docs/conduct_capability_policy_july09.doc

3 Governance

Certain aspects of information security are governed by legislation, namely ;

The Data Protection Act (1998)

The General Data Protection Regulations (2018)

The Computer Misuse Act (1990)

The Copyright, Designs and Patents Act (1988)

Aspects of these pieces of legislation can be found within the Policy. Further information can be found at Appendix A and the legislation in full can be found at www.legislation.gov.uk.

4 Roles and Responsibilities

The Director – Technology & Corporate Programmes & Data Protection Officer has responsibility for managing organisational information risk, setting strategic direction and ensuring policies and processes are in place for the safe management of information assets.

Corporate Management Team and Heads of Service have responsibility for understanding and addressing information risk within their directorates, assigning ownership to information assets and ensuring that appropriate arrangements are in place to manage information risk, and provide assurance on the security and use of those information assets.

Information Asset Owners undertake risk assessments, implement controls, recognise potential and actual security incidents and ensure that policies and processes are followed.

All managers must ;

- Be aware of any ICT equipment being used outside of Council premises for the purposes of site visits or home / remote working and ensure staff are aware of the associated security requirements
- Ensure all staff are instructed in their security responsibilities, including undertaking mandatory training
- Ensure staff are fully trained in the use of computer systems
- Determine the levels of access to IT systems for each member of staff, based on job role and function, irrespective of status
- Ensure that system administrators are advised in a timely manner regarding staff changes affecting system access so that passwords can be withdrawn or changed as appropriate
- Ensure that the Clear Desk Policy is enforced, particularly in relation to confidential or personal information

Managers and Staff must ;

- Ensure that no breaches of information security result from their own actions
- Report any suspected or actual information breach without delay. The notification process can be found at Appendix B
- Undertake all mandatory training pertaining to information security, understanding that by not doing so could result in network accounts being suspended and the invocation of disciplinary proceedings under the Councils Disciplinary Procedure

5 INFORMATION PROCESSING

5.1 Privacy by Design

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. While currently good practice, the General Data Protection Regulations (GDPR) which come into force in May 2018, introduce a legal requirement for privacy impact assessments and privacy by design in certain circumstances.

The council will, therefore, ensure that privacy and data protection is a key consideration in the early stages of any project, and subsequently throughout its lifecycle.

Core privacy considerations should be incorporated into existing project management and risk management methodologies and policies to ensure:

Potential problems are identified at an early stage
Increased awareness of privacy and data protection
Legal obligations are met and data breaches are minimised
Actions are less likely to be privacy intrusive and have a negative impact on individuals

Privacy Impact Assessments (PIAs) are an integral part of taking a privacy by design approach. Guidance on undertaking a PIA can be found on InfoZone
http://infozone.tamworth.gov.uk:901/data-protection-impact-assessments

5.2 Data Breaches and Information Security Incidents

The council has a duty to ensure that all personal information is processed in compliance with the principles set out in the Data Protection Act, and subsequently General Data Protection Regulations. It is ultimately the responsibility of each Head of Service to ensure that their service areas comply with that duty and that suitable procedures are in place for staff to follow when dealing with personal information.

The Data Protection Principles and General Data Protection Regulation Principles can be found at Appendix C

A data breach could be defined as the unintentional release of personal or sensitive personal information to an unauthorised person, either through accidental disclosure or loss/theft. However, non-compliance with any of the Principles referred to at Appendix C could be classed as a breach, particularly if there is a possibility that the data subject could be put at risk or suffer substantial damage or distress.

A security incident is defined as a breach of council security which may result in a risk of loss, access to or corruption of council information or assets, whether personal or not.

Examples of data breaches and security incidents, including the notification process, can be found at Appendix B

In the event of any breach or security incident, it is vital that action is taken to minimise any associated risk to either the council or its customers as soon as possible.

It is important that all staff are aware of their responsibilities when handling personal information, keeping it secure and not disclosing it without proper cause. Suitable information handling procedures should be in place and all staff must undertake mandatory Data Protection training on an annual basis. Officers found not to have under-taken mandatory training will have their network access suspended and may be subject to disciplinary proceedings under the Council's Conduct and Capability Policy.

Similarly, staff must be alert to the possibility of cyber-attacks or phishing attempts.

In order to keep Members of the Audit and Governance Committee informed, it is agreed that serious breaches involving personal information, where the decision is made to report to the Information Commissioner's Office (ICO), will be reported to the next available meeting of the Committee. The Committee will also receive a copy of any decision reached by the ICO following its investigation into the breach.

5.3 Payment Card Industry (PCI) Compliance

The Council is currently working towards PCI DSS compliance. The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all companies that process, store or transmit credit or debit card information maintain a secure environment.

Failure to comply with these standards could lead to fines or even the removal of the Councils ability to accept card payments.

Those users who have access to any part of the Councils Cash Receipting systems whereby they are taking payments either in person or over the phone should only enter Card numbers into the relevant payment screens and **under no circumstances** should Card Holder data such as Card Numbers be written down, copied by anybody or read aloud as this would breach PCI compliance.

5.4 Retention and Disposal of Information

Information must only be retained for as long as it is needed for business purposes, or in accordance with any statutory retention period

Staff should refer to the council's Information Retention Policy for further information. The Schedule sets out the type of information held in service areas, together with statutory or agreed retention periods. Please contact the Data Protection Team for further advice on retention at data-protection@tamworth.gov.uk. Detail of the Data Protection Team can be found at Appendix D.

When disposing of information please ensure the most appropriate method is used. Paper files containing personal or sensitive information must be disposed of in the confidential waste bins. Electronic information must be permanently destroyed

When purchasing new computer systems or software, please consider requirements for the retention and disposal of information and ensure these are included at the scoping stage

All information destroyed in accordance with the Retention Schedule must be logged on the Information Asset Register

5.5 Cloud Storage Solutions

The use of cloud storage solutions (Skydrive, Onedrive Personal, iCloud etc.) for the transfer of council information is expressly forbidden. Information Services can provide you with access to its secure Onedrive for Business for the sharing of files.

Where Cloud Storage is considered as part of a technical solution to an Invitation to Tender, Information Services must be consulted to ensure compatibility and security

5.6 Systems Development

All system developments must comply with the council's ICT & Digital Strategy. All system developments must include security issues in their consideration of new developments, seeking guidance from Information Services , where appropriate.

Privacy Impact Assessments (PIAs) should be carried out prior to the purchase of any new system which will be used for storing and accessing personal information. Guidance on PIAs can be found on InfoZone

5.7 Data Back-up

Data should be held on a network directory where possible, to ensure routine backup processes capture the data. Information must not be held on a PC hard drive

Data should be protected by clearly defined and controlled back-up procedures which will generate data for archiving and contingency recovery purposes.

Information Services and all other systems administrators should produce written backup instructions for each system under their management. The backup copies should be clearly labelled (physically and/or electronically) and held in a secure area. Procedures should be in place to recover to a useable point after restart of this back-up.

Archived and recovery data should be accorded the same security as live data and should be held separately preferably at an off-site location. Archived data is information which is no longer in current use, but may be required in the future, for example, for legal reasons or audit purposes. The council's Retention Policy must be followed in determining whether data should be archived.

Recovery data should be sufficient to provide an adequate level of service and recovery time in the event of an emergency and should be regularly tested.

To ensure that, in an emergency, the back-up data is sufficient and accurate, it should be regularly tested. This can be done by automatically comparing it with the live data immediately after the back-up is taken and by using the back-up data in regular tests of the contingency plan.

Recovery data should be used only with the formal permission of the data owner or as defined in the documented contingency plan for the system.

If live data is corrupted, any relevant software, hardware and communications facilities should be checked before using the back-up data. This aims to ensure that back-up data is not corrupted in addition to the live data. An engineer (software or hardware) should check the relevant equipment or software using his/her own test data.

5.8 Equipment, Media and Data Disposal

If a machine has ever been used to process personal data as defined under the Data Protection Act (1998) or General Data Protection Regulations (2018) or 'in confidence' data, then any storage media should be disposed of only after reliable precautions to destroy the data have been taken. Procedures for disposal should be documented on the council's Information Asset Register.

Many software packages have routines built into them which write data to temporary files on the hard disk for their own purposes. Users are often unaware that this activity is taking place and may not realise that data which may be sensitive is being stored automatically on their hard disk.

Although the software usually (but not always) deletes these files after they have served their purpose, they could be restored and retrieved easily from the disk by using

commonly available utility software. Therefore, disposal must be arranged through Information Services who will arrange for disks to be wiped or destroyed to the appropriate standards.

5.9 Software

All users should ensure that they only use licensed copies of commercial software. It is a criminal offence to make/use unauthorised copies of commercial software and offenders are liable to disciplinary action. Each user should ensure that a copy of each licence for commercial software is held.

The loading and use of unlicensed software on council computing equipment is **NOT** allowed. All staff and members must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove the software was legally acquired. The council monitors the installation and use of software by means of regular software audits; any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the council's Conduct and Capability Policy.

The council will only permit authorised software to be installed on its PCs. Approval will be via Information Services.

Where the council recognises the need for specific specialised PC products, such products should be registered with Information Services and be fully licensed

Software packages must comply with, and not compromise, council security standards.

Computers owned by the council are only to be used for the work of the council. The copying of leisure software on to computing equipment owned by the council is not allowed. Copying of leisure software may result in disciplinary action under the council's Disciplinary Policy. Computer leisure software is one of the main sources of software corruption and viruses which may lead to the destruction of complete systems and the data contained on them.

Educational software for training and instruction should be authorised, properly purchased, virus checked and loaded by Information Services staff or its authorised representatives. Where a software training package includes 'games' to enable the new user to practise their keyboard skills e.g. Windows, then this will be allowed as long as it does not represent a threat to the security of the system.

The council seeks to minimise the risks of computer viruses through education, good practice/procedures and anti-virus software positioned in the most vulnerable areas. Users should report any viruses detected/suspected on their machines immediately to Information Services at ICTServiceDesk@tamworth.gov.uk

Users must be aware of the risk of viruses from email and the internet. If in doubt about any data received please contact Information Services for anti-virus advice.

6 INFORMATION SHARING

6.1 Posting or Emailing Information

If information is particularly sensitive or confidential the most secure method of transmission must be selected. The following procedures should be adopted as appropriate, depending on the sensitivity of the information.

Consider the risk of harm or distress that could be caused to the customer if the information was lost or sent to another person, then look at the most appropriate way of sending the information to the recipient.

It is important that only the minimum amount of personal or sensitive information is sent, by whichever method is chosen. However, email should always be the default method selected with subsequent methods used only where there is no email option.

Sending information by email:

- Carefully check the recipient's email address before pressing send
- Check the full content of the email, particularly where forwarding an email you have received from someone else. Ensure it is appropriate to forward the whole message
- Take care when replying 'to all' – do you know who all recipients are and do they all need to receive the information you are sending
- If emailing sensitive information, password protect any attachments. Use a different method to communicate the password eg telephone call, messenger or text.
- Consider the use of secure email where this is available
- Person identifiable data files **must not** be sent via email to a user's personal mail box. Staff working from home should only access information via the council's network.

Sending information by post:

- Wherever possible, the iMail or PSL solution should be used
- Check that the address is correct
- Ensure only the relevant information is in the envelope and that someone else's letter hasn't been included in error

- If the information is particularly sensitive or confidential, discuss the most secure method of delivery with the Post room, this could be by Recorded, Special Delivery or even courier.

- Refer to the Post Policy for additional information regarding the sending of information by post

Printing and Photocopying:

- All printing must be via the MFP printers or an external contracted supplier
- Consideration must be given to using external printing facilities for large print runs, especially where personal information is concerned
- When printing or photocopying multiple documents, ensure you separate them when you return to your desk. This will minimise the risk of the wrong documents being processed incorrectly
- If the copier jams please remove all documents – if the copier remains jammed report it, but leave your contact details on the copier so that once it has been fixed any remaining copying can be returned to you. If possible, cancel your print run
- Make sure your entire document has copied or printed – check that the copier has not run out of paper. This is particularly important when copying or printing large documents. Please bear in mind the printer will sometimes pause in the middle of a large print run
- Do not leave the printer unattended when you're using it – someone else may come along and pick up your printing by mistake

6.2 Redacting

If it is necessary to redact information, either before sending it out or posting it onto the website, ensure a suitable and permanent redaction method is used

The use of black marker pen is **not** a suitable method of redaction

It is not advisable to change the colour of text (eg white text on a white background) or use text boxes to cover text as these can be removed from electronic documents. However, if this is the only option, once redacted the document should be printed and then scanned as a PDF before being sent.

6.3 Sharing and Disclosing Information

When disclosing personal or sensitive information to customers, particularly over the phone or in person, ensure you verify their identity. Service areas dealing with customers on a daily basis should have suitable security questions which must always be used. If in doubt ask for suitable ID or offer to post the information (to the contact details you have on file)

If a request for disclosure of information is received from a third party, you must:

- Obtain written consent from the customer that they are acting on their behalf
- Verify their identity, particularly if they request information via the telephone or in person. It is preferable to telephone the person back, using a recognised telephone number for their organisation (for example 101 for the Police). Do not take their mobile number and use that.
- In all circumstances, you must ensure you are legally able to share the information being requested and only share the minimum amount of information necessary.

If at any time you are unsure, contact the Data Protection Team at data-protection@tamworth.gov.uk

7 INFORMATION CONTROLS

7.1 Access control

Staff, Elected Members, contractors and staff working under IR35 arrangements should only access systems for which they are authorised. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems for which they have no authorisation. All contracts of employment and conditions of contract for contractors should have a non-disclosure clause, which means that in the event of accidental unauthorised access to information (whether electronic or manual), the member of staff or contractor is prevented from disclosing information which they had no right to obtain.

Formal procedures will be used to control access to systems. An authorised manager must raise an IT Service Request via the ICT ServiceDesk for each application for access. Access privileges will be modified/removed - as appropriate - when an individual changes job or leaves. Managers must ensure they advise IT of any changes requiring such modification/removal.

Staff, Elected Members, contractors and staff working under IR35 arrangements must comply with the council's Acceptable Use Policy.

When a member of staff leaves the employment of the council, both a Termination of Employment form and a Leavers – IT Access Removal form must be completed by their manager and forwarded onto HR. This will ensure relevant teams are informed and access to the council's network, email and buildings is removed.

In addition to the above, line managers must ensure that passwords to local systems are removed or changed to deny access. This would apply where, for example, the system is externally hosted and not under the remit of Information Services.

Particular attention should be paid to the return of items which may allow future access. These include ICT equipment, mobile phones, personal identification devices, access cards, keys, passes, manuals & documents. Where endpoint security is deployed to personal devices, access will be removed by Information Services.

The timing of the above requirements will depend upon the reason for the termination, and the relationship with the employee. Where the termination is mutually amicable, the removal of such things as passwords and personal identification devices may be left to the last day of employment.

Once an employee has left, it can be impossible to enforce security disciplines, even though legal process. Many cases of unauthorised access into systems and premises can be traced back to information given out by former employees.

Prior to an officer leaving, it is good practice for a meeting to be held during which the manager notes all the systems to which the member of staff has access and informs the relevant system administrators of the leaving date. Special care needs to be taken when access to personal, commercially sensitive or financial data is involved.

Managers must ensure that staff leaving the council's employment do not inappropriately wipe or delete information from hard disks. If the circumstances of leaving make this likely then access rights should be restricted to avoid damage to council information and equipment.

All visitors should have official identification issued by the council. If temporary passwords need to be issued to allow access to confidential systems these need to be disabled when the visitor has left. Visitors should not be afforded an opportunity to casually view computer screens or printed documents produced by any information system without authorisation.

There is a requirement for system administrators to have a procedure in place for the secure control of contractors called upon to maintain and support computing equipment and software. The contractor may be on site or working remotely via a communications link. Information Services can advise on the most suitable control.

Physical security to all office areas is provided through the access control system. Staff should challenge strangers in the office areas without an ID badge. Never let someone you don't know or recognise to tailgate you through security doors.

Refer to the Building Use Policy for additional information regarding physical security

7.2 Security of Equipment

Portable computers must have appropriate access protection, for example passwords and encryption, and must not be left unattended in public places.

Computer equipment is vulnerable to theft, loss or unauthorised access. Always secure laptops and handheld equipment when leaving an office unattended and lock equipment away when you are leaving the office.

Due to the high incidence of car thefts laptops or other portable equipment must **never** be left unattended in cars or taken into vulnerable areas. The organisation's insurance does not cover equipment stolen from vehicles.

Users of portable computing equipment are responsible for the security of the hardware and the information it holds at all times on or off council property. The equipment should only be used by the individual to which it is issued, be maintained and batteries recharged regularly.

Staff working from home must ensure appropriate security is in place to protect council equipment or information. This will include physical security measures to prevent unauthorised entry to the home, ensuring council equipment and information is kept out of sight and ensuring other household members are not able to see Council information.

Council issued equipment must not be used by non-council staff unless contractually obliged to do so, such as agency staff

All of the policy statements regarding the use of software and games apply equally to users of portable equipment belonging to the council.

Users of portable equipment away from council premises should check their car and home insurance policies for their level of cover in the event of equipment being stolen or damaged and take appropriate precautions to minimise risk of theft or damage.

Staff and Elected Members who use portable computers belonging to the council must use them solely for business purposes otherwise there may be a personal tax/National Insurance liability.

7.3 Security and Storage of Information

All information, whether electronic or manual, must be stored in a secure manner, appropriate to its sensitivity. It is for each service area to determine the sensitivity of the information held and the relevant storage appropriate to that information. Suitable storage and security will include:

- Paper files stored in lockable cupboards or drawers
- Laptops stored in lockable cupboards or drawers
- Electronic files password protected or encrypted
- Restricted access to ICT systems
- Computer screens to be 'locked' whenever staff leave their desk

Removable media to be kept in lockable cupboards or drawers and information deleted when no longer required

Paper files removed from the office (for site visits or when working from home) to be kept secure at all times.

Laptops and paper files must **never** be left in unattended vehicles

It is advisable that paper files containing personal or sensitive data are kept separate from laptops, particularly when working from home

At no time should sensitive, confidential or personal information be stored on a portable unit's hard drive. Access to this type of information must always be through the council's network.

Staff should be aware of the position of their computer screens and take all necessary steps to prevent members of the public or visitors from being able to view the content of computers or hard copy information

7.4 Clear Desk Policy

Employees are required to clear working documents, open files, and other paperwork from their desks, working surfaces and shelves at the end of each working day and to place them securely into desk drawers, cupboards and lockers as appropriate.

Although security measures are in place to ensure only authorised access to office areas, employees should ensure that documents, particularly of a confidential nature are not left lying around.

Employees must ensure that documents are carefully stored. When properly implemented, this clear desk policy also improves efficiency as documents can be retrieved more easily.

7.5 Vacating Premises or Disposing of Equipment

It is important that a process is in place to ensure all council information is removed from premises should they be vacated and from equipment before it is disposed of. Equipment includes cupboards and filing cabinets as well as computers or other electronic devices.

ICT equipment must be returned to Information Services to be appropriately disposed of.

If the council vacates any of its premises, the manager of the service area occupying the premises must undertake appropriate checks of all areas, including locked rooms, basements and other storage areas, to ensure all council information is removed. Such checks should be documented, dated and signed.

If information is bagged for disposal (whether confidential or not), this must be removed before the building is vacated.

The organisation's Disposal Policy must be adhered to at all time.

7.6 Network Security

The council will engage a third-party specialist to routinely review network security as part of its annual penetration testing. Results and subsequent actions from these tests are presented to Corporate Management Team

7.7 Risks from Viruses

Viruses (including malware and zero day threats) are one of the greatest threats to the council's computer systems. PC viruses become easier to avoid with staff and members aware of the risks with unlicensed software or bringing data/software from outside the council. Anti-virus measures reduce the risks of damage to the network.

Information Services centrally maintain and update the currency of the virus definition files on servers, but users are responsible for checking that virus updates are automatically occurring on all desktop machines. Advice and support is available from Information Services if any remedial action is necessary. Any suspected virus attacks must be reported to the ICT ServiceDesk

7.8 Cyber Security

Cyber security and cybercrime are increasing risks that, if left unchecked, could disrupt the day to day operations of the council, the delivery of local public services and ultimately have the potential to compromise national security.

Further information regarding Cyber Security can be obtained from Information Services.

7.9 Access Control to Secure Areas

Secure areas include:

- The post room
- The ICT server room

All central processors/networked file servers/central network equipment will be located in secure areas with restricted access.

The council's central computer suite is a high security area housing corporate computer systems. An entry restriction system is in place to protect the suite.

Local network equipment/file servers and network equipment will be located in secure areas and where appropriate within locked cabinets.

Unrestricted access to the central computer facilities will be confined to designated staff whose job function requires access to that particular area/equipment.

Restricted access may be given to other staff where there is a specific job function need for such access.

Authenticated representatives of third party support agencies will only be given access through specific authorisation for a specified period of time

All secure areas will have an entry log which staff and visitors must use.

Regular reviews of who can access these secure areas should be undertaken.

7.10 Security of Third Party Access

No external agency will be given access to any of the council's networks unless that body has been formally authorised to have access.

All external agencies processing personal information on the council's behalf (including via a hosted IT system) will be required to sign a third party processing agreement.

The council will control all external agencies access to its systems by enabling/disabling connections for each approved access requirement.

The council will put in place adequate policies and procedures to ensure the protection of all information being sent to external systems. In doing so, it will make no assumptions as to the quality of security used by any third party but will request confirmation of levels of security maintained by those third parties. Where levels of security are found to be inadequate, alternative ways of sending data will be used.

All third parties and any outsourced operations will be liable to the same level of confidentiality as council Staff.

7.11 Use of Removable Media

It is the council's policy to prohibit the use of all unauthorised removable media devices. The use of removable media devices will only be approved if a valid business case for its use is developed.

All staff, Members and third parties must comply with the requirements regarding removable media which can be found in the ICT Policy

7.12 Timeout Procedures

Inactive computers should be set to time out after a pre-set period of inactivity. The time-out facility should clear the screen. The time-out delay reflects the potential security risks of unauthorised access.

Users must 'lock' their computers, if leaving them unattended for any length of time. For high risk applications, connection time restriction should be considered. Limiting the period during which the computer has access to Information Services reduces the window of opportunity for unauthorised access

7.13 System Documentation

All systems should be adequately documented by the system manager and should be kept up to date so that it matches the state of the system at all times.

System documentation, including manuals, should be physically secured (for example, under lock and key) when not in use. An additional copy should be stored in a separate location which will remain secure, even if the computer system and all other copies are destroyed.

Distribution of system documentation should be formally authorised by the system manager. System documentation may contain sensitive information, for example, descriptions of applications processes, authorisation processes.

Manual data covered by the Gov Connect (GCSX) must not be removed from the council offices in accordance with the agreement.

APPENDIX A - LEGISLATION

Data Protection Act (1998)

Further information can be found at www.legislation.gov.uk

The Data Protection Act 1998 came into force in March 2001, replacing the Data Protection Act 1984. It provides individuals with important rights, including the right to find out what personal information is held about them

The EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. The Data Protection Act is how the UK implements the European Directive.

Anyone who processes personal information must comply with the eight principles as detailed in Appendix C.

The Data Protection Act makes the Information Commissioner responsible for:

- promoting good practice in handling personal data, and giving advice and guidance on data protection;
- keeping a register of organisations that are required to notify him about their information-processing activities; and
- helping to resolve disputes by deciding whether it is likely or unlikely that an organisation had complied with the Act when processing personal data.

If an individual believes they have been the victim of a breach of the Data Protection Act they can complain to the ICO. The ICO will make a judgement as to whether it is ‘likely’ or ‘unlikely’ that the Data Protection Act has been breached.

The ICO can also conduct assessments to check organisations are complying with the Act and serve information notices requiring organisations to provide the ICO with specified information within a certain time period.

They can also serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law.

General Data Protection Regulations (2018)

Further information can be found at www.ico.org.uk

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

The GDPR applies to 'controllers' **and** 'processors'. The definitions are broadly the same as under the DPA – ie the controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are currently subject to the DPA, it is likely that you will also be subject to the GDPR.

If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR. However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.

Personal data

Like the DPA, the GDPR applies to 'personal data'. However, the GDPR's definition is more detailed and makes it clear that information such as an online identifier – eg an IP address – can be personal data. The more expansive definition provides for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

For most organisations, keeping HR records, customer lists, or contact details etc, the change to the definition should make little practical difference. You can assume that if you hold information that falls within the scope of the DPA, it will also fall within the scope of the GDPR.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – eg key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

Sensitive personal data

The GDPR refers to sensitive personal data as “special categories of personal data” (see Article 9). These categories are broadly the same as those in the DPA, but there are some minor changes.

For example, the special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Under the GDPR, the data protection principles set out the main responsibilities for organisations.

The principles are similar to those in the DPA, with added detail at certain points and a new **accountability** requirement. The GDPR does not have principles relating to individuals’ rights or overseas transfers of personal data - these are specifically addressed in separate articles.

The most significant addition is the accountability principle. The GDPR requires you to show **how** you comply with the principles – for example by documenting the decisions you take about a processing activity. This is explained in greater detail later in this guide.

Article 5 of the GDPR requires that personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against

accidental loss, destruction or damage, using appropriate technical or organisational measures.

For processing to be lawful under the GDPR, you need to identify a lawful basis before you can process personal data. These are often referred to as the “conditions for processing” under the DPA. It is important that you determine your lawful basis for processing personal data and document this. This becomes more of an issue under the GDPR because your lawful basis for processing has an effect on individuals’ rights. For example, if you rely on someone’s consent to process

Consent under the GDPR must be a freely given, specific, informed and unambiguous indication of the individual’s wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent. Public authorities and employers will need to take particular care to ensure that consent is freely given.
Consent has to be verifiable, and individuals generally have more rights where you rely on consent to process their data.

The GDPR creates some new rights for individuals and strengthens some of the rights that currently exist under the DPA. The GDPR provides the following rights for individuals:

1. The right of access
2. The right to rectification
3. The right to erasure
4. The right to restrict processing
5. The right to data portability
6. The right to object
7. Rights in relation to automated decision making and profiling.
8. The right to be informed

Computer Misuse Act (1990)

Further information can be found at www.legislation.gov.uk

The Computer Misuse Act was passed in 1990 to recognise offences caused by hacking.

The Computer Misuse Act (1990) recognised :

- Unauthorised access to computer material
- Unauthorised access with intent to commit or facilitate a crime
- Unauthorised modification of computer material.
- Making, supplying or obtaining anything which can be used in computer misuse offences.

Unauthorised access to computer material

This is the lowest level of offence and is one that many of us might be guilty of at some stage of our working lives. Have you ever logged onto someone else's network account? If you do this and then look at their files, even if you don't change, delete or damage anything, you are still guilty of accessing materials without authorisation - and this is illegal.

This offence carries the risk of being sentenced to six months in prison and/or a hefty fine.

Unauthorised access with intent to commit or facilitate a crime

The difference between this and the first offence is that the person gaining access to someone else's system is doing so with the sole purpose of doing something illegal.

This might mean that they had to guess or steal the password in order to get into someone's user area or their bank account. They could do this by trial and error or by using special programs such as spyware or keylogging software, or they could use a relatively new technique called 'phishing'.

They might want to steal some company secrets or they might want to transfer some money out of your bank account into their own.

Anyone caught doing this risks up to a five year prison sentence and/or a hefty fine.

Unauthorised modification of computer material

Everyone deletes files from their own system, maybe they no longer need them or maybe they delete them by mistake. This is fine - there was no intent to cause any damage.

This offence relates to the deletion or changes made to files with the intent to cause damage to an individual or company. The difference is *'the intent to cause damage'*.

This offence also covers purposely introducing viruses to other peoples' systems.

If you knowingly transmit a virus to others, you are guilty under this section of the Computer Misuse Act.

This offence carries a penalty of up to five years in prison and/or a fine.

Making, supplying or obtaining material that could be used in computer misuse offences

Making

This includes the writing or creation of computer viruses, worms, trojans, malware, malicious scripts etc.

Supplying

This part covers the distribution of any of the above material whether you have created it yourself or obtained it from elsewhere. It is an offense to supply or distribute these files to others.

Obtaining

If you purposely obtain malicious files such as as computer viruses or scripts that you know could be used to damage computer systems then you have committed an offence under the Computer Misuse Act.

This part of the Act is known as 3A.

Copyright, Designs and Patents Act (1988)

Further information can be found at www.legislation.gov.uk

This Act states that it is illegal to copy and use software without the copyright owner's consent or the appropriate licence to prove that the software was legally acquired.

All software purchased will have an appropriate licence agreement which will have a different approach to licencing ;

- Individual Licence
- Network Licence
- Concurrent Licence
- Site Licence

All users must be aware of the type of licencing they are purchasing through engagement with Information Services.

Any infringement or breach of software copyright may result in legal proceedings by the software author or distributor.

APPENDIX B – NOTIFICATION PROCESS AND EXAMPLES OF DATA BREACHES

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority. The organisation must do this within 72 hours of becoming aware of the breach, where feasible.

If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, the organisation must also inform those individuals without undue delay.

The organisation must also keep a record of any personal data breaches, regardless of whether they fall into the requirement to notify.

Examples of data breaches include ;

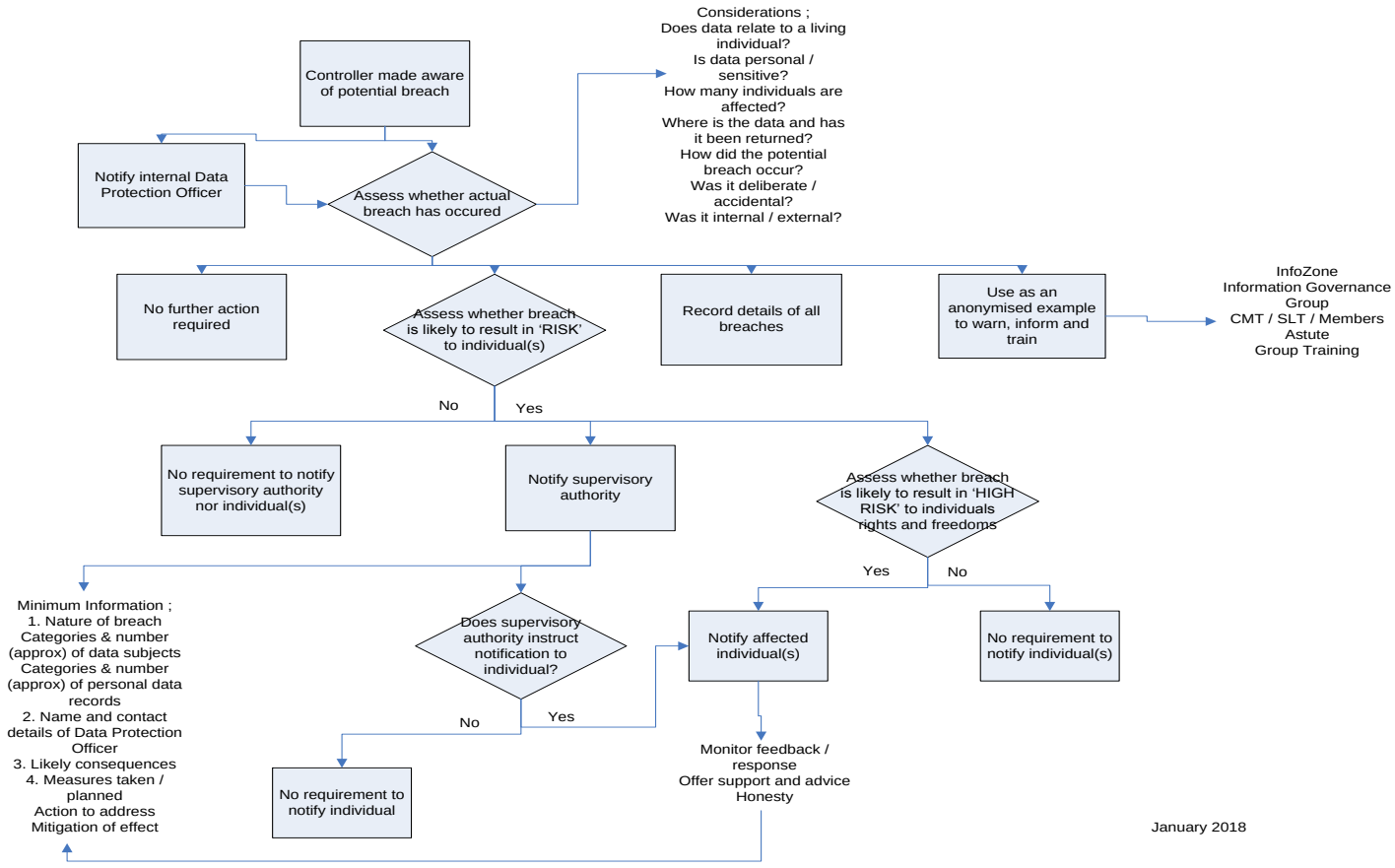
- Loss of paperwork containing names, addresses and health details
- Correspondence being sent to wrong recipient by post, email or fax
- Theft of a laptop
- Conversation regarding a vulnerable adult taking place in a public place and being overheard
- Papers left in a meeting room after completion of the meeting

If you suspect a potential or actual information breach, notify the organisation's Data Protection Officer or Deputy immediately

- Data Protection Officer – Nicki Burton, Director Technology & Corporate Programmes 01827 709420
- Deputy Data Protection Officer – Nikkie Hesketh, Project and Information Co-Ordinator 01827 709266
- Data-protection@tamworth.gov.uk

On notification of a potential or actual breach, the following process will be followed ;

Data Breach Notification Process



APPENDIX C – DATA PROTECTION AND GENERAL DATA PROTECTION REGULATIONS PRINCIPLES

DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

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 those 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 or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects 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 country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

GENERAL DATA PROTECTION PRINCIPLES

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

APPENDIX D – DATA PROTECTION TEAM DETAILS

Nicki Burton – Data Protection Officer

Director – Technology & Corporate Programmes

Nicki-burton@tamworth.gov.uk

01827 709420

Nikkie Hesketh – Deputy Data Protection Officer

Project and Information CoOrdinator

Nicola-hesketh@tamworth.gov.uk

01827 709266