NORTH WARWICKSHIRE BOROUGH COUNCIL

DATA PROTECTION POLICY

April 2018

Data Protection Policy

1. Introduction

1.1 North Warwickshire Borough Council is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act") and the changes arising from the General Data Protection Regulation (GDPR) and in the Data Protection Act 2018..

1.2 We will, therefore, follow appropriate policy and procedures to ensure that all our employees, Councillors and others working on our behalf, who have access to or process any personal information held by us, or on our behalf, are made aware of their duties and responsibilities under the Act and the new requirements specified in the GDPR and the Data Protection Act 2018.

1.3 This document is our Data Protection Policy, which has been reviewed in April 2018 as part of the preparations for the implementation of the General Data Protection Regulation and the Data Protection Act 2018. The revised policy will be reported to the Council's Executive Board for adoption on 18 June 2018. It will be subject to review at three yearly intervals or earlier, if circumstances require this to be done, for example, changes in legislation or to our structure or policies.

1.4 The Data Protection Policy sets out the overarching policies and procedures for the information governance framework for the Council. The policy sets out the Council's commitment and approach to data protection and provides a clear frame of reference for employees to determine our standards, aims, and objectives for data protection compliance. The policy's objectives are:

- To provide a clear frame of reference for employees to determine our standards, aims, and objectives for data protection compliance.
- To provide information to data subjects, data processors, and the regulatory authorities about how the Council approaches data protection compliance.

1.5 The policy takes into account the findings from an external review of the compliance with the General Data Protection Regulation requirements carried out in December 2017.

2. Legal Background

2.1 The General Data Protection Regulation 2016 (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. The Government have set out in a Data Protection Act 2018 some provisions for how the GDPR will apply in the UK. The requirements of GDPR are enforceable by the Information Commissioner's Office from the 25 May 2018.

2.2 The GDPR applies to personal data, which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

2.3 There are other data protection related laws which are relevant to this policy including the Privacy and Electronic Communications Regulations 2003, the Freedom of Information Act 2000, the Protection of Freedoms Act, the Common Law Duty of Confidentiality, Data Retention and Investigatory Powers Act 2014, Computer Misuse Act 1990, Human Rights Act 1998 and others. The Council will endeavour to ensure that the appropriate legislation is followed in all its policy and procedures relating to personal data.

3. **Statement of Policy**

3.1 The Council is committed to compliance with all relevant Data Protection Legislation and will ensure that all its employees and organisations working on its' behalf are following the appropriate policy and procedures to comply with the legislation and our owned defined standards for data protection and information governance.

3.2 This policy document sets out how the Council intends to implement appropriate controls and procedures sufficient to ensure legal compliance. The policy document will be reviewed to ensure that legal standards are being met adequately as they change over time and that compliance is being met. The Council will ensure that all employees and any organisations acting on behalf of the Council that process personal data have received appropriate training in the application of this policy and the relevant legislation.

3.3 The Council's Management Team will ensure that sufficient and appropriate resources are available to ensure that the legal requirements relating to data protection legislation and the standards set out in this policy are met.

3.4 The Council's Management Team will ensure that the Services provided by or on behalf of the Council will follow the six data protection principles which are set out below and personal data shall be:

1. Processed fairly, lawfully and in a transparent manner in relation to the data subject.
2. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. Accurate and, where necessary kept up to date.
5. Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
6. Processed in a way 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.

3.5 The controls and measures that the Council will use to ensure compliance with the six data protection principles will include keeping sufficient records of our data processing activities, risk assessments and decisions.

3.6 The Council will uphold the rights and freedoms of people applicable to them by the Data Protection Legislation. The rights and freedoms will be appropriately taken into account in the decisions we take which may affect people and will ensure there are sufficient controls in place to assist people to exercise their rights.

3.7 This policy applies to all of the Council's activities and functions which involve the processing of personal data. The policy applies to anyone who is involved in processing personal data for or on behalf of the Council including employees, casual and temporary staff, sub contractors, suppliers, volunteers and anyone who the Council shares or discloses personal data with or to.

3.8 In order to operate efficiently, we have to collect and use personal data about people with whom we work. These may include members of the public; current, past and prospective employees; service users; contractors, agents, consultants and suppliers. We may also be required by law to collect and use information in order to comply with the requirements of Government Departments and Agencies.

3.9 All personal information must be handled and dealt with properly no matter how it is collected, recorded and used and whether it is held on paper, in computer records or recorded by any other means. There are safeguards in the Act which ensure this.

3.10 We will, therefore, make certain that we treat all personal information that we hold in a lawful and correct manner and in accordance with the Act. We will also comply with the Data Protection Principles set out in the Act (see below).

4. **Responsibilities**

4.1 *Data Controller and Data Processor*

4.1.1 North Warwickshire Borough Council is a legal data controller and processor under the Data Protection Legislation.

4.2 *Management and Supervisory Staff*

4.2.1 The Chief Executive is the accountable officer responsible for the management of the Council and ensuring appropriate mechanisms are in place to support service delivery and continuity. Protecting data and maintaining confidentiality is a key responsibility for the Council in how it operates.

4.2.2 Each Assistant Chief Executive or Assistant Director in their respective areas of responsibility must ensure that all staff members are aware of this policy, other relevant policies and procedures, and their responsibilities concerning the processing of personal data. They must ensure this policy is adhered to. Managers and supervisory staff are responsible for ensuring that all data processing operations under their control or sphere of responsibility or commissioned by them are undertaken in compliance with this policy and other relevant data protection policies. They are responsible for ensuring that anyone processing data is sufficiently aware of this policy and how it applies to their job role and sufficiently trained to carry out their duties in compliance with this policy.

4.3 *Senior Information Risk Officer(SIRO*)

4.3.1 The role of a Senior Information Risk Officer is part of the current role of the Assistant Director Corporate Services to lead and implement the information governance risk assessment programme and advise the Executive Board on the effectiveness of information risk management across the Council.

4.4 *Data Protection Officer*

4.4.1 The Data Protection Officer role is part of the responsibilities of the Assistant Chief Executive & Solicitor to the Council. The role is responsible for providing the policies, guidance and training needed to ensure the Council is both compliant with Data Protection Legislation and risk assessed. The Data Protection Officer will monitor and report to the Council's Management Team in respect of compliance with this policy, investigate any breaches, and maintain suitable records of processing activities. They

may co-opt other individuals to assist with the management of data protection obligations.

4.4.2 The DPO is responsible for monitoring the evolution of the Data Protection Legislation, case law, guidance, and codes of practice and incorporating relevant changes into the Council's policy.

4.5 *Employees, volunteers, casual/temporary workers, directors and officers etc***.**

4.5.1 Anyone who is directly employed by the Council to undertake data processing activities including but not limited to employees, volunteers, casual/temporary workers, directors and officers involved in the receipt, handling or communication of personal data must adhere to this policy. Anyone who is not confident in or has concerns about data handling practices that they are undertaking or witnessing should contact the Data Protection Officer. Individuals are expected to complete appropriate training from time to time. Everyone within the Council has a duty to respect data subjects' rights to confidentiality.

4.5.2 Disciplinary action may be taken against staff for non-compliance with relevant policies and legislation.

4.6 *Partner & Third-Party Responsibilities*

4.6.1 Any Third Party or Organisation that is commissioned to process data or receives data from the Council, or is able to access any personal data **must** enter into a legally enforceable agreement with the Council the nature of which will be determined by the level of involvement with the data that is held, shared or accessed. Any such agreement must be approved by the DPO.

5.1 **Policy Detail**

5.1.1 **Fair Lawful and Transparent processing**

5.1.2 The processing of all personal data by the Council will only be undertaken in a fair, lawful and transparent manner meaning:

Fairness – no data collection activities will be undertaken or commissioned without an appropriate privacy notice being provided to the person from whom data are being collected and to the people who the data are about if personal data are collected from sources other than the data subject. All privacy information and any changes to privacy information must be approved by the DPO.

Lawfulness – no data collection activities will be undertaken or commissioned without there being a lawful ground for the data processing activities intended to be applied to the personal data. The DPO is responsible for determining the lawful grounds for processing. Where the lawful grounds are consent, the consent policy will apply. Where the lawful grounds are legitimate interests, a legitimate interests assessment (LIA) will be undertaken and documented. The information process owner is responsible for ensuring that there are lawful grounds for all data processing activities that fall under their sphere of control, that the consent policy is adhered to and a LIA is properly undertaken where necessary. The DPO will provide advice regarding lawful processing conditions.

Transparency – the Council will endeavour to provide sufficient information about how personal data are being processed to enable sufficient transparency about its handling of personal data. The DPO is tasked with periodically reviewing the apparent transparency.

5.2 Data processing purposes

5.2.1 Personal data will only be collected, created or otherwise obtained for specific, explicit and legitimate purposes. No data processing will be undertaken or commissioned without the approval of the DPO who shall maintain a register of data processing activities and their purpose. Data process owners are responsible for ensuring that all of the data processing activities that they undertake and/or commission have been approved by the DPO. No personal data will be used for any purpose other than that which it was collected and/or created for without the approval of the DPO.

5.3 Data minimisation

5.3.1 The Council will strive to use a minimum of personal data in its data processing activities and will periodically review the relevance of the information that is collected. Data process owners are responsible for ensuring that no un-necessary, irrelevant or unjustifiable personal data are collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in. The DPO will provide advice regarding the justification of personal data collected or created.

5.4 Data accuracy

5.4.1 The Council recognises that the accuracy of data is important and that some data is more important to keep up-to-date than others. The Council will use its reasonable endeavours to maintain data as accurate and up-to-date as possible, in particular data which would have a detrimental impact on data subjects if it were inaccurate or out-of-date. Data process owners are responsible for ensuring that personal data they have collected or created either directly or indirectly through the data processing activities they are responsible for and/or engage in are maintained accurate and up to date and that personal data whose accuracy cannot reasonably be assumed to be accurate and up to date are treated appropriately through erasure or anonymisation. The DPO will provide advice regarding data accuracy.

5.5 Data retention

5.5.1 The Council will ensure that it does not retain personal data for any longer than is necessary for the purposes for which they were collected and will apply appropriate measures at the end of data's useful life such as erasure or anonymisation. Data process owners will be responsible for determining the retention period for personal data under control or sphere of influence and the DPO will maintain a data retention schedule setting out approved retention periods and end of life treatment. The DPO must approve all retention periods for personal data. Because data retention is a vitally important issue as both the over-retention and under-retention of personal data could have a detrimental impact on both the data subject and the Council the DPO will undertake regular data retention audits.

5.6 Information security

5.6.1 The Council will ensure that any personal data that it processes or commissions the processing of is 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. The Council will endeavour to use an electronic information processing approach whenever possible to do so. In particular an information security management policy (ISMP) will be maintained setting out specific policies in relation to maintaining personal data secure, confidential, available and with integrity. The Assistant Director Corporate Services will be responsible for the formulation of the Information Security Management Policy and must consult the DPO in regard to it. The DPO is authorised to challenge the ISMP and is required to report any concerns to the Council's Management Team that they may have about it.

5.7 Record keeping and accountability

5.7.1 In order to fulfil its responsibility to be able to demonstrate compliance with Data Protection Legislation as well as in support of the policy on transparency the Council will maintain records of the processing activities that it controls, undertakes or otherwise commissions as required by the Data Protection Legislation and specifically those required in Article 30 of the GDPR.

5.8 Information rights

5.8.1 The Council recognises the legal rights of those whose data it is processing or intends to process and will ensure that appropriate information is provided to them advising them of their rights, and that policies and procedures are maintained to ensure that the organisation is able to recognise information rights requests and handle them appropriately when they are exercised.
These rights include:

- Right to information about data processing operations
-
- Right of access to personal data
- Right to portability of personal data
- Right of rectification of personal data
- Right of erasure of personal data
- Right to restriction of processing
- Right to object to direct marketing
- Right to object to data processing operations under some circumstances
- Right not to be subject to decisions made by automated processing under some circumstances
- Right of complaint about the organisation's processing of personal data and the right to a judicial remedy and compensation

5.9 **Consent**

5.9.1 The Council will interpret consent to be as defined in the GDPR and that any consent shall not be valid unless:

- there is a genuine choice;
- it has been explicitly and freely given, and represents a specific, informed and unambiguous indication of the data subject's wishes that signifies agreement to the processing of personal data relating to them;
- the consent was given through statement made by the data subject or by a clear affirmative action undertaken by them;
- the organisation can demonstrate that the data subject has been fully informed about the data processing to which they have consented and is able to prove that it has obtained valid consent lawfully;
- a mechanism is provided to data subjects to enable them to withdraw consent and which makes the withdrawal of consent in effect as easy as it was to give and that the data subject has been informed about how to exercise their right to withdraw consent;

5.9.2 The Council recognises that consent may be rendered invalid in the event that any of the above points cannot be verified or if there is an imbalance of power between the data controller and the data subject. The Council recognises that consent cannot be considered to be forever and will determine a consent refresh period for every instance where consent is the lawful condition for processing.

5.10 **Personal Data Breaches**

5.10.1 The Council will maintain a Data Breach Reporting Procedure and will ensure that all employees and those with access to personal data are aware of it and this breach reporting policy. All employees and individuals with access to personal data for which the organisation is either data controller or processor must report all personal data breaches to an appropriate individual as set out in the Data Breach Reporting Procedure as soon as they become aware of the breach. The organisation will log all personal data breaches and will investigate each incident without delay. Appropriate remedial action will be taken as soon as possible to isolate and contain the breach, evaluate and minimise its impact, and to recover from the effects of the breach. Data protection near misses will also be recorded and investigated in the same manner as data protection breaches. The breach reporting procedure will set out responsibilities, decision-making criteria and timescales for notifying data subjects, the Information Commissioner and the media about a personal data breach.

5.11 **Data Processors**

5.11.1 The Council reserves the right to contract out data processing activities or operations involving the processing of personal data in the interests of business efficiency and effectiveness. No third party data processors will be appointed who are unable to provide satisfactory assurances that they will handle personal data in accordance with the Data Protection Legislation. People wishing to appoint a data processor will ensure that appropriate due diligence is undertaken on the proposed data processor in the field of information governance and data protection compliance prior to their appointment. The DPO will provide advice and guidance in respect of this. A written agreement will be implemented between the Organisation and the data processor which at least meets the requirements of the Data Protection Legislation. The DPO will ensure that a register of such agreements/arrangements is maintained. The data

processor agreement will specify what is to happen to personal data upon termination of the data processing agreement.

5.11.2 No employee is permitted to commission or appoint a third party to process data on behalf of the Council without adhering to this policy.

5.12 **Data sharing, disclosure and transfer**

5.12.1 The Council will only share personal data with or otherwise disclose personal data to other organisations and third parties where there is a legal basis for doing so and the data sharing is necessary for specified purposes. No data sharing or disclosure is permitted to occur without a suitable legally enforceable agreement satisfying the requirements for such agreements as set out in the Data Protection Legislation being in place. Data sharing agreements must be approved by the DPO who will maintain a register of all such agreements. Appropriate risk assessments will be undertaken prior to any data sharing taking place on those with whom we intend to share personal data. This policy extends to appointing others to process personal data on our behalf, sharing personal data with organisations, and providing information to ad hoc requests for information such as those which may be received from the police and other authorities.

5.12.2 The Council will provide information to all employees setting out safe and approved methods of transferring personal data to recipients. Employees are required to use only approved methods of data transfers. Disciplinary action will be taken against employees who fail to observe the data transfer policy and use unsafe and insecure methods of data transfer unless such methods have been approved in writing by the DPO.

5.13 **Internationalisation of personal data**

5.13.1 The Council will neither transfer nor process nor will it permit personal data to be transferred or processed outside the United Kingdom without the conditions laid down in the Data Protection Legislation being met to ensure that the level of protection of personal data are not undermined.

5.13.2 Any transfer or processing of personal data that the organisation undertakes or commissions whether directly or indirectly must be approved by the DPO and may only take place if one of the following is satisfied:

- The territory into which the data are being transferred is one approved by the UK's Information Commissioner;
- The territory into which the data are being transferred is within the European Economic Area;
- The territory into which the data are being transferred has an adequacy decision issued by the European Commission;
- The transfer is to the United States of America and the recipient is registered under the EU/US Privacy Shield scheme;
- The transfer is made under the unaltered terms of the standard contractual clauses issued by the European Commission for such purposes;
- The transfer is made under the provision of binding corporate rules which have been approved and certified by the European Commission;
- The transfer is made in accordance with one of the exceptions set out in the Data Protection Legislation.

5.14 **Risk Assessment**

5.14.1 The Council will embrace the principles and foster a culture of privacy by design and by default. It will maintain a policy requiring data protection impact assessments (DPIA) to be undertaken and documented and ensure that appropriate resources are available to advise on DPIAs. The DPO is responsible for maintaining a risk register of data protection compliance risks that have been identified by the organisation and for its periodic review.

5.15 **Children's data**

5.15.1 Special measures will be taken by the Council if it processes personal data relating to children under the age of 13 including the nature of privacy information provided and approach to information rights requests. These special measures will be set out in a policy relating to children's data.

5.16 **Training and awareness**

5.16.1 The Council will ensure that all those who it engages to process personal data either directly or indirectly are provided with appropriate training in the application of this and other data protection policies and procedures and in their data protection responsibilities. It will also undertake data protection awareness raising activities from time to time to keep data protection front of mind. All training and awareness raising activities will be logged. Refresher training will be provided periodically.

5.17 **Audit and compliance checking**

5.17.1 The Council will undertake periodic compliance checks to test whether its policies and procedures are being adhered to and to test the effectiveness of its control measures. Corrective action will be required where no-conformance is found. Records will be kept of all such audits and compliance checks including corrective action requests raised. Disciplinary action will be taken against individuals who fail to act upon the reasonable corrective action requests properly formulated and raised through data protection audits. The Board of Directors will be provided with a summary of audit findings periodically

6 **Glossary**

Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

Data Processor
means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Data subject
any living individual who is the subject of personal data held by an organisation;

Data Process Owner
The person responsible for the instigation or on-going maintenance of a data process or data processing operation;

Personal data
means any information relating to an identified or identifiable living individual;

Identifiable living individual
means a living individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual;

Special Categories of Personal Data
means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

Processing
means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Information Incident
means an identified occurrence or weakness indicating a possible breach of information security or failure of safeguards, or a previously unknown situation which may be relevant to the security of information;

Personal Data Breach
means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Risk
The chance of something happening, which will have an impact upon objectives. It is measured in terms of consequence and likelihood;

Risk Management
The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects;

Senior Information Risk Owner (SIRO)
An Executive Director or member of the Senior Management Board with overall responsibility for the Organisation’s information risk strategy;

Corporate Data
Corporate data relates to any sensitive corporate information including meeting schedules, agendas and minutes of meetings; financial accounts; contracts; and organisational policies and procedures.

Recipient
means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of

those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

Third party
Means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

Profiling Is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual;

Consent
Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data;

	Document Control and approval			
Issue	Description of Change	Approval	Date of Issue	Status
Version 1.0	Revised policy for GDPR compliance	Management Team 01/05/18		

This policy will be disseminated to key staff groups as below:
Management Team – communication directly by email and discussion at Management Team meeting
Assistant Directors and Principal Officers - communication directly by email and discussion at Extended Management Team meeting and team meetings
All staff - Organisational communication channels, all new starters will be made aware of this Policy as part of their induction process. Managers will be responsible for keeping staff up-to-date with any changes to this Policy.

Approval
Name
Position
Signature:
Date:

Appendix

Data Security Tips

- Staff should only have access to information they need to do their job
- Passwords should not be shared
- Encrypt any personal information held electronically if it will cause damage or distress if it is lost or stolen
- Shred all confidential paper waste
- Train staff so that they are aware of what is expected of them
-

The Information Commissioner's Office recommends the following security measures to protect personal information which the Council has taken into account in developing our data security measures and policy.

For computer security:

- Install a firewall and virus-checking on your computers. ✓In place.
- Make sure that your operating system is set up to receive automatic updates. ✓In place.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities. ✓In place.
- Only allow your staff access to the information they need to do their job and don't let them share passwords. ✓In place.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen. ✓This is our practice for information taken off site.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information. ✓In place.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk). ✓In place.
- Consider installing an anti-spyware tool. Spyware is the generic name given to programs that are designed to secretly monitor your activities on your computer. Spyware can be unwittingly installed within other file and program downloads, and their use is often malicious. They can capture passwords, banking credentials and credit card details, then relay them back to fraudsters. Anti-spyware helps to monitor and protect your computer from spyware threats, and it is often free to use and update. ✓In place.

For using emails securely:

- Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.
- When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc).

When you use cc every recipient of the message will be able to see the address it was sent to.

- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

For using faxes securely:

- Consider whether sending the information by a means other than fax is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. For example, if a solicitor asks you to forward a statement, send only the statement specifically asked for, not all statements available on the file.
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers.
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office.
- If the fax is sensitive, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine.
- Ring up or email to make sure the whole document has been received safely.
- Use a cover sheet. This will let anyone know who the information is for and whether it is confidential or sensitive, without them having to look at the contents.

For other security:

Shred all your confidential paper waste. ✓The Council uses a waste collection service which takes our paper waste to be incinerated. Should this practice be reviewed?

Check the physical security of your premises. ✓Our buildings have a number of security arrangements including restricted door access, alarms and other measures. Should they be reviewed as part of the current accommodation project?

Data Policy Note
During the course of carrying out work duties staff should adhere to the following guidelines:
1. Try to eliminate taking paper records off site particularly information containing personal data
2. If paper records containing personal information have to be taken off site only take what is essential. For example only take specific information you need and not a complete file.
3. When off site don't leave paper records unattended, for example left in a car, customer's property or in your property. (Note copies of major emergency plan can be kept at home in a secure situation).
4. Don't keep paper records off site longer than absolutely necessary.
5. Don't disclose any information to anyone that you have no legal basis to do so.

6. If taking more than one file off site use separate folders if possible and not see through plastic wallets. This will help eliminate the risk of someone viewing information that they are not allowed to.