NORTH EAST LINCOLNSHIRE COUNCIL www.nelincs.gov.uk	Internal Ref:	NELC 16.60.05
	Review date	December 2016
	Version No.	V04

Confidentiality Policy

1 Introduction

a) The purpose of this policy is to introduce the concept of confidentiality for the processing of information by North East Lincolnshire Council. This policy will raise awareness of the importance of confidentiality and set out a framework for the processing of sensitive information by those acting on behalf of North East Lincolnshire Council.

b) Sensitive information can include;

- Personal Information;
- Sensitive Personal Information;
- Commercially Sensitive Information; or
- Sensitive Corporate Information.

c) We believe that everyone has a fundamental right to the information held about them being kept secure and confidential.

d) Officers acting on behalf of the Council, will have authority to obtain and disclose personal data, but they will be committing a criminal offence if they use this position to obtain, disclose, or procure disclosure of personal data for their own purposes.

e) Everyone acting on behalf of the Council (Officers) are expected to:

- Treat all personal and sensitive information as confidential to the authority, whether the information has been received formally, informally or discovered by accident;
- Comply with the law regarding the protection and disclosure of information;
- Only disclose personal information where there is a justified purpose and in accordance with the Data Protection Act; and
- Not gain or attempt to gain access to information they are not authorised to have.

f) The North East Lincolnshire Council Terms and Conditions of Employment stipulate the confidentiality clause officers are bound to comply with.

2 Scope

a) This policy applies to everyone acting on behalf of North East Lincolnshire Council including Elected Members and employees, whether permanent, temporary or contracted, either as an individual or through a third party supplier, thereafter known as Officers.

b) The Council is fully committed to the broad principles of social justice and is opposed to any form of discrimination or oppression, and will act at all times in accordance with its Equality Scheme. Link to the Council's Diversity and Equality Policies

3 Legal Framework

a) The work of the Council requires the collection, use and disclosure of information for a variety of purposes, this processing is subject to the following legislation:

1. The Human Rights Act (1998) - Article 8 guarantees the right to respect for privacy and family life, home and correspondence.
2. The Data Protection Act (1998)- requires that any personal information collected by and used within the Authority be processed fairly and lawfully.
3. The common law duty of confidence requires that the public expectations of confidentiality be respected. Link to the Council's Data Protection Policy
4. The Caldicott Initiative identifies a need to ensure that confidentiality is respected throughout the process of care.
5. The Public Interest Disclosure Act (1998) Public Interest Disclosure Act, which allows exemptions for specific kinds of disclosure by employees, such as the raising of concerns of practice.
6. The Freedom of Information Act (2000) – Provides a general right of access to the information held by the Council. Link to the Council's Freedom of Information Policy

4 Responsibilities within North East Lincolnshire Council

a) The Senior Management Team is responsible for ensuring that this policy is implemented, monitored and adhered to across all service areas.

b) The Information Security and Assurance Board are responsible for raising awareness of this policy and providing advice and guidance in relation to this policy.

c) HR Group Manager is responsible for overseeing the Disciplinary Policy and procedures.

d) Everyone acting on behalf of North East Lincolnshire Council must be aware of, understand and comply with the requirements of this policy and appropriate legislation when handling or processing information. Challenge and report inappropriate behaviour or breaches of this policy.

5 How to Keep Information Confidential

5.1 Overview

a) All information should be classified and handled in accordance with the Council's policies and procedures.

b) Only authorised officers should process confidential information.

c) Confidential information must not be disclosed, discussed or viewed in public or unsecure areas.

d) The processing of information should be evidenced.

5.2 Processing Information

a) Processing of information must be in accordance with relevant legislation and the Council's policies and procedures. For Personal and Sensitive Personal Information this must be in accordance with the Data Protection Act. The principles of the Act state that personal data shall

1. Be processed fairly and lawfully and shall not be processed unless at least one of the conditions specified in Schedule 2 of the Act (and Schedule 3 in relation to sensitive personal data) are met;
2. Be obtained for one or more specified and lawful purpose and shall not be processed in any manner incompatible with that purpose;
3. Be adequate, relevant and not excessive for those purposes;
4. Be accurate and, where necessary, kept up to date;
5. Not be kept for longer than is necessary for that purpose;
6. Be processed in accordance with the rights of the data subject;
7. Be kept secure from unauthorised or unlawful processing and protected against accidental loss, destruction or damage by using the appropriate technical and organisational measures; and
8. 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.

b) Unless an exemption applies Data Subjects must be fully aware of the purpose for which their information will be processed, and give their informed consent for the processing.

c) Where an individual is incapable of giving consent to process their information, due to limitations of age or mental capacity, consent will be sought from an appropriate Guardian, such as a parent, next of kin, individual with power of attorney, or agency with guardianship responsibility (such as the Local Authority acting in the role of corporate parent for Looked after Children).

5.3 Disclosing Information

a) The Council can receive spurious or false requests for information. Officers must therefore take all reasonable steps to verify the identity of the requester. Requests should normally be made in writing or through secure networks.

b) Personal or Sensitive Personal Information must only be shared with partner agencies and other organisations for specific purposes, with the informed consent of the Data Subject, unless there is an appropriate exemption under the Data Protection Act.

c) Personal information relating to deceased individuals will continue to be treated as confidential and will not be disclosed without clear justification. The privacy and wishes of relatives will be taken into account when considering the appropriateness of such disclosures. Wishes expressed by a Data Subject prior to their death will be respected.

d) Data Subjects have a right to be provided with their own personal information (Subject Access Request) under the Data Protection Act unless an exemption applies, for example:

1. To share the information is deemed a risk of harm;
2. A third party has not supplied consent (where consent is deemed necessary);
3. It would be prejudicial to law enforcement or the assessment/collection of Council Tax; or
4. It would be prejudicial to the conduct of the Councils regulatory functions.

5.4 Accessing Information

a) Officers must only have access to the systems, equipment and information that they genuinely need to carry out their work, and will respect the confidentiality of that information at all times.

b) Officers must never view or amend information, about themselves, their family or friends. If authority has been given to the Officer to act on behalf of someone else then this should be done through the same channels as other customers i.e. through the contact centre or customer access points.

c) If an Officer inadvertently accesses a case or account which relates to someone they know, they should immediately notify their line manager so that an appropriate record of access can be made.

d) In all cases where an Officer has an interest in a claim, property or account, or where there may be a conflict of interest, a declaration of interest should be completed so that system access is blocked where appropriate. It is the responsibility of the Officer to inform their line manager of any conflict of interest or any changes to that declaration of interest.

5.5 Physical Security

a) Confidential Information must be kept in a secure environment. With controlled access to building and rooms, and use of lockable filling cabinets or drawers.

b) The clear desk policy must be followed. Information must be put away securely when not in use.

c) Confidential information must never be left unattended.

d) When transferring confidential information it must always be passed to the authorised Officer, it must never be left on their desk or other unsecure places.

e) All confidential information must be disposed of appropriately and in accordance with the Council Records Management Policy / ICT and Information Security Standards. Confidential information or equipment (i.e. encrypted USBs) containing confidential information must not be placed in normal waste bins or recycling bins.

f) ID badges must be worn at all times.

5.6 For Transportation of information

a) Confidential information must never be taken out of a secure environment, without a justified reason.

b) Where confidential information is taken out of a secure environment, it must be signed out and back in.

c) Before taking confidential information out of a secure environment, always consider if it can be summarised or anonymised.

d) If confidential information and equipment does leave the office it must be kept secure at all times, and returned to a secure environment as soon as possible

e) Confidential information and equipment must never be left unattended on public transport, personal transport or in public areas.

f) Where confidential information is outside of the secure environment overnight, it must be stored in a secure location within the Officer's home.

5.7 Use of Equipment

a) Council issued equipment must remain secure at all times and never left unattended.

b) Council issued equipment must only be used by Council Officers.

c) Council issued equipment must wherever possible be encrypted and password protected.

d) Passwords must comply with the Council's requirements, and be kept secure at all times.

5.8 Faxing

a) Fax machines must only be used to transmit confidential information in exceptional circumstances, where no other form of communicating of the information is available. When using a Fax machine employees must follow the procedure set out in the ICT and Information Security Standards.

5.9 USBs

a) Only encrypted USB memory sticks issued by the Council ICT section may be used or connected to the Council's network.

5.10 Telephone and Private Conversations

a) Officers should not disclose confidential information over the telephone unless they have satisfied themselves as to the identity of the requester and are in a secure environment to prevent information being overheard by others.

b) When answering the telephone consider where you are positioned and who is around you. If unauthorised people (for that piece of information) are around you then find somewhere more private to take the call.

5.11 Emails

a) When sending confidential information via email always use a secure e-mail account.

b) Always check the recipient's e-mail address before sending, to avoid releasing confidential information to unauthorised personnel. Send a test e-mail if required.

5.12 Social Media

a) No confidential information must ever be published onto any social media sites.

5.13 Data used for training purposes

a) Confidential data shall not be used for training purposes, always use anonymised data.

6 Breaches of Policy

a) Breaches of the confidentiality policy may constitute Gross misconduct and will be investigated under the Council's disciplinary procedure. The unauthorised disclosure of personal information is an offence under the Data Protection Act (1998).

b) Any confidential information which is obtained accidentally must be reported immediately or at the next appropriate time, otherwise you may be seen to breach this policy resulting in a disciplinary procedure.

c) If you are found to have obtained confidential information for personal gain it will result in a disciplinary procedure and possible court action for criminal misconduct.

d) Details of the measures in place and the responsibilities of officers including the immediate notification of the ICT Advanced Practitioner (Security & Compliance) can be found in this policy and the ICT and Information Security Standards.

7 Review of Policy

a) This policy will be reviewed 2 yearly unless otherwise required by legislation changes or issues identified in operational practice.

b) The review of this policy will be undertaken by Information Security and Assurance Board.

8 Definitions

For further clarification on terms used in this policy please see the table below;

Term	Definition
Data Subject	The person(s) the personal information is about.
Processing	Collecting, using, disclosing, retaining or disposing of information.
Officers	Everyone acting on behalf of North East Lincolnshire Council including Elected Members and employees, whether permanent, temporary or contracted, either as an individual or through a third party supplier.
Anonymised	The removal of all personal and/or confidential data from the information
Personal Information	Information where a living individual can be identified, either on its own or with information that is already in possession of an organisation or can likely come into possession of an organisation
Sensitive personal information	Personal Information containing information about an individual's • Race/ Ethnic Origin • Political opinions • Religious beliefs/ beliefs of a similar nature • Trade Union Membership • Physical/Mental Wellbeing • Sexual Preferences or Sex life • Any alleged offences • Criminal Record
Commercially Sensitive Information	Information which if disclosed could prejudice the ability of North East Lincolnshire Council or a third party to effectively conduct its commercial activities.
Sensitive Corporate Information	Information which if disclosed could prejudice the ability of North East Lincolnshire Council to effectively conduct its activities.