North Hykeham Town Council

ICT Policy

1. What is Information and Communication Technology?

Information and Communication Technology (ICT) is loose term which is used to describe a wide range of tools and techniques, usually electronic in nature, which speed up and/or aid communication.

North Hykeham Town Council recognises the importance of embracing ICT in order to ensure that its customers benefit from efficient levels of service delivery.

2. Aims

The Council supports the Government's aim of improving electronic access to public services. The aims of this policy are to:

- facilitate the ongoing development of the efficient management and delivery of the Council's services;
- provide opportunities for staff to acquire and develop core ICT competencies;
- ensure that the Council's ICT systems are reviewed regularly and adjusted to meet new or changing need, including legislative changes.

3. Management

The Town Clerk has overall responsibility for ICT and the implementation of this policy.

4. Technical Support

The Town Council shall appoint an independent and competent ICT support provider, which will be subject to a 3-year review in order to confirm the service they provide meets service delivery needs.

5. Security

a) Individuals shall:

- be responsible for their Town Council's user names and passwords;
- protect user credentials against misuse;
- not share or disseminate any user credentials with another person;
- only attempt to access ICT where permissions have been given;
- not misuse or alter the configuration or settings of any ICT;
- not attempt to bypass or subvert ICT security controls;
- not introduce unofficial software, hardware, removable media or files without appropriate authorisation;

- not leave a computer system open if it is unattended;
- operate a clear screen policy when you leave ICT unattended, for example by temporary "locking" the computer;
- protect all ICT portable media and devices at all times, in particular when transporting them outside of Council premises

b) All ICT media and portable devices used to process Council information shall be password protected and encrypted.

c) Prevent inadvertent disclosure of personal or sensitive information by avoiding being overlooked when working

d) Take care when printing information and carefully check the distribution list for any material to be transmitted.

e) Securely store or destroy any printed material which contains private information, sensitive, disclosive or identifiable records or that which is not for public circulation.

f) Staff and Members shall report any security incident or suspected security incident to the Town Clerk as soon as is reasonably possible.

6. Hardware

The Town Council's computer systems and computer peripherals will be subject to annual review in order to confirm that they are meeting service delivery needs.

All computers and computer peripherals will be listed, and revisions/deletions will be assessed for upgrade or replacement. The Town Council operates a 3-year rotational replacement programme for its essential services computers. All other computers and computer peripherals will be reviewed over a 3-year period.

7. Telephones and related systems

The Town Council currently is contracted to a digital cloud-based telephone system, including the hire of equipment; this practice will be subject to contractual review by the Town Clerk and the Finance and Policy Committee in order to confirm that this meets service delivery needs and is cost-efficient. All telephone and related systems will be assessed over a 3-year period and assessed for replacement / repair where necessary.

Except in exceptional circumstances, use of the telephone, related and electronic communication systems must be used for legitimate business purposes only. Personal use must be authorised by the Town Clerk.

Employees may be provided with a mobile telephone in order to assist with the proper performance of their duties. The mobile telephone remains the property of the Council and the Council may withdraw its use. It must be returned to the Council on the termination of employment. The mobile telephone is the responsibility of the employee and if it is lost, they will be responsible for the replacement cost.

Employees are not permitted to make and receive personal telephone calls/texts on any mobile telephone issued to them by the Council, without authorisation by the Town Clerk. If the Council

considers that there has been improper use of the mobile telephone, employees may be required to meet the cost of any calls that are not business related and such costs may be deducted from their remuneration.

Calls and texts on personal mobile phones should wherever possible be restricted to formal rest breaks.

8. Software

The Town Council's computer software will be subject to review every 3 years in order to confirm that it is meeting service delivery needs and demand.

9. Internet access

The Town Council provides a public Wi-Fi access, the details of which are listed in the Civic Offices. Access to the Town Council's secure Internet must be approved by an authorised user, usually the Town Clerk or Deputy Town Clerk.

- Access to the Internet for 'leisure' purposes is permitted during authorised break times.
- Access for personal reasons is permitted in certain circumstances, however it is the responsibility of the 'user' to ensure no illegal or prohibited sites are accessed; should this happen by error a report should be immediately submitted to the Town Clerk.

10. e-mail

The Council requires that the Town Council's civic offices and The Community Hub to have the capability of sending/receiving email messages and data. All councillors are required to use their allocated email address for all correspondence relating to town council matters.

Members of staff, elected members and authorised users shall ensure:

- e-mail use must be lawful and inoffensive;
- they do not send personal or sensitive data over public networks such as the Internet unless an approved method of protection or encryption has been applied to it;
- they check that the recipients of e-mail messages are correct so that personal, or sensitive information is not accidentally released into the public domain;
- personal or business email accounts shall not be used to conduct Council business;
- personal use of the Internet shall be reasonable, proportionate and occasional and shall not interfere with the performance of their role or the performance of the system;
- they do not use Town Council e-mail address(es) to send personal emails unless the item is marked as 'personal' and the sender clearly identifies that communication as such.

11. Unacceptable use of ICT

Members of staff, elected members and authorised users shall ensure:

- any security incident or suspected security incident is reported to the Town Clerk as soon as is reasonably possible;
- personal or business email accounts are not to be used to conduct Council business;

- they do not communicate information via an ICT system knowing it or suspecting it to be unacceptable within the context and purpose for which it is being communicated;
- they do not process or access racist, sexist, defamatory, offensive, illegal or otherwise inappropriate material;
- they do not carry out illegal, fraudulent or malicious activities;
- they do not store, process or displaying offensive or obscene material, such as pornography or hate literature;
- they do not annoy or harass another individual, for instance by sending chain letters, uninvited e-mail of a personal nature or by using lewd or offensive language;
- they do not break copyright;

12. Remote Access

The Town Council recognises that staff may need to work from remote locations from time to time. To address this issue, provision for remote access is available. Log on and password information will be issued to staff members. Staff members shall report any security incident or suspected security incident to the Town Clerk as soon as is reasonably possible.

13. Personal Data

Any member of staff processing personal data must comply with the eight enforceable principles of good practice (Data Protection Act 1988 & 2003).

These stipulate that data must be:

a) fairly and lawfully processed;

b) processed for limited purposes;

c) adequate, relevant and not excessive;

d) accurate;

e) not kept longer than necessary;

f) processed in accordance with the data subject's rights;

g) secure;

h) not transferred to countries without adequate protection.

14. Data Protection

a) Confidentiality

Passwords are to be used to restrict access to personal and/or confidential data. If there is any doubt about whether access to certain data should be restricted, guidance should be sought from the Town Clerk.

b) Viruses

All computers used to send/receive emails or to access the Internet must have recognised anti-virus software installed. No disk, drive or memory stick from any external source shall be opened until it has been checked for viruses.

c) Back-ups

The Town Council's server system will back-up the system's current data files at the end of each working day, with a full download once a week to a cloud-based storage

15. Training

The Town Council recognises that training staff and councillors using new technology products is essential. Therefore:

a) all users of IT office productivity facilities (such as word processing and spreadsheets) shall be given appropriate training;

b) adequate training in the use of specialised or bespoke software packages will be given to all users of that software;

c) training will be given to users of any new software as part of the implementation programme.

16. Awareness

Individuals shall make themselves aware of, and comply with, requirements and legislation regarding information security and data protection along with any other legal, statutory or contractual obligations identified by the Town Council.

17. Monitoring

The Town Council reserves the right to monitor or record all communication systems including email, electronic messaging and internet use. Records of activity may be used by the organisation for the following purposes:

- quality assurance
- conduct
- discipline
- performance
- capability and/or criminal proceedings and any other purpose compliant with the regulatory and legislation framework in force and useful to support the Council's business activities.

18. Breaches of Policy

All Council employees have a contractual responsibility to be aware of and conform to the Council's values, rules, policies and procedures. Breaches of policy may lead to disciplinary proceedings.

Individuals who fail to comply with the Council's policies and who are not Council employees may have their access to Council information and ICT revoked and such action could have impacts on contracts with third party organisation.