Fakenham Connect
Oak Street
Fakenham
Norfolk
NR21 9DY
Tel: 01328 853653
e-mail: info@fakenhamtowncouncil.gov.uk
website: fakenhamtowncouncil.gov.uk

Fakenham Town Council

Information Transfer Policy

CONTENTS:

1. Purpose

There are many occasions when information is transferred between departments, to third-party service providers, to other public bodies, commercial organisations and individuals. This is done using a wide variety of media and methods, in electronic and paper format.

In every transfer, there is a risk that the information may be lost, misappropriated or accidentally released. Fakenham Town Council has a duty of care in handling information.

This policy forms part of the Council's Digital Governance Framework and must be read in conjunction with the following related policies:

- IT Policy (Core Digital Governance Framework)
- Councillor Email Policy
- Removable Media Policy
- Social Media and Communications Policy
- Data Protection Policies
- Records Management and Retention Policy

- Members' Code of Conduct

The IT Policy provides the overarching framework for digital security, acceptable use, monitoring, and incident management. Supporting policies provide operational or role-specific guidance and must not contradict the IT Policy.

Where overlap exists between policies, the requirements of the IT Policy shall take precedence.

Failure to comply with any of the above policies may result in formal action in accordance with the Council's disciplinary procedures and, where applicable, statutory obligations under the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Freedom of Information Act 2000.

2. Scope

The scope of this policy covers any type of information (i.e. word documents, PDF reports and excel spreadsheets) in any format and on any medium.

This policy applies to all employees, Councillors and authorised third-parties handling Council information.

3. Exclusions

This policy does not cover the transfer of information over the internal network, which has its own automated security controls. It does not cover proprietary secure transfer mechanisms such as BACS financial transfers that have their own separately implemented security requirements.

4. Roles and Responsibilities

Proper definitions of roles and responsibilities are essential to assure compliance with this Policy. In summary these are:

4.1 The Sender

The Sender is responsible for ensuring the following requirements of this Policy are met.

- Assessing the information to be sent, in-line with the Risk Assessment section of this policy.
- Ensuring that the identity and authorisation of the recipient has been formally confirmed and documented.
- Obtaining the consent of the Information Asset Owner for the transfer.
- Ensuring that the information is sent and tracked in an appropriate manner.

4.2 Employees

Individual employees will be responsible for familiarising themselves with this Policy and ensuring that any information transfer for which they are responsible is done in a compliant manner.

Any suspected or actual breach during information transfer must be reported immediately in-line with the Incident Response Policy and the Council's IT Policy Section 12.

5. Risk Assessment

Consider the following before transferring information. If in doubt, please contact the Clerk.

Is the transfer legal and necessary?

1. It is dangerous to assume that because someone asks for information that they are necessarily authorised or legally entitled to have it. If you are in doubt then you should check with Fakenham Town Council
2. Once you are sure that the transfer is legal and necessary, then you must decide what kind of information you are dealing with. This will determine what security is appropriate.

3. To transfer personal or confidential information without these checks may leave Fakenham Town Council open to legal and reputational damages and the sender may be subject to disciplinary action.

Is it personal information?

Personal information is about a living, identifiable individual. If it contains details of racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health, sexual life, commission of offences, court appearances and sentences it is further classified as sensitive personal information. Anything we do with personal information must comply with the Data Protection Act 2018 and General Data Protection Regulation (GDPR).

Before you make any transfer, you must:

- Ensure that the transfer is legal (under the Data Protection Act & GDPR).
- Ensure that the transfer is necessary (is there a less intrusive way).
- Remove or blackout anything that is not essential for the recipient's purpose.
- Have a documented agreement in place to ensure the recipient understands their responsibilities under the law, particularly what to do with the transfer file after they have extracted the information to their system.

Is it confidential information?

Confidential information is that which Fakenham Town Council has a duty of confidentiality. This may include information that affects the business interests of a third party, or for which the sender does not hold copyright e.g. bank details, salary details, contracts, agreements.

Before you transfer you must:

- Ensure that you are not breaching a Non-Disclosure Agreement.
- Ensure that the transfer is necessary (is there a less intrusive way).
- Remove anything that is not essential for the recipient's purpose.
- Have a documented agreement in place to ensure the recipient understands their responsibilities under the law, particularly what to do with the transfer file after they have extracted the information to their system.

6. Electronic Mail & Encrypted Links

- Any password used must adhere to Password Management Policy.
- Any password to open the attached file must be transferred to the recipient using a different method than e-mail. ~~Consideration must be given.~~
- E-mail message must contain clear instructions on the recipient’s responsibilities and instructions on what to do if they are not the correct recipient.
- An accompanying message and the filename must not reveal the contents of the encrypted file.
- Check with the recipient that their e-mail system will not filter out or quarantine the transferred file.
- All electronic transfers must comply with the Council’s IT Policy (Sections 4, 6, 8, and 11) regarding device security, encryption, password management, and secure messaging.
- Senders must verify receipt of transferred information and ensure it is securely retained in accordance with IT Policy Sections 7 (Monitoring) and 11 (Social Media, Messaging, and AI Tools) and report any issues to their line manager.

6.1 Electronic memory (CD, DVD, Flash media drive)

Information must be stored encrypted using a product approved by an approved mechanism according to the Encryption policy.

- Any password used must adhere to Password Management Policy.
- Any password or key to open the attached file must be transferred to the recipient using a different method than e-mail, e.g. a telephone call to an agreed telephone number, closed letter.
- An accompanied message must contain clear instructions on the recipient's responsibilities and instructions on what to do if they are not the correct recipient.
- An accompanying message and the filename must not reveal the contents of the encrypted file.
- Senders must verify receipt of transferred information and ensure it is securely retained in accordance with IT Policy Sections 7 (Monitoring) and 11 (Social Media, Messaging, and AI Tools) and report any issues to their line manager.

6.2 Delivery by Post or by Hand

- It is essential that the file, whether electronic or paper is kept secure in transit, tracked during transit, and delivered to the correct individual.
- An appropriate delivery mechanism must be used.
- Package must be securely and appropriately packed, clearly labelled and have a seal, which must be broken to open the package.
- Package must have a return address and contact details.
- The label must not indicate the nature or value of the contents.
- Package must be received and signed for by addressee.
- Senders must verify receipt of transferred information and ensure it is securely retained in accordance with IT Policy Sections 7 (Monitoring) and 11 (Social Media, Messaging, and AI Tools) and report any issues to their line manager.

6.3 Telephone/Mobile Phone

- Transferred information must be kept to a minimum.
- Personal or Confidential information must not be transferred over the telephone unless the identity and authorisation of the receiver has been appropriately confirmed.
- When transferring information via telephone or messaging apps, users must follow security requirements in IT Policy Section 11, including confidentiality, secure storage, and proper authorisation.

Reviewed at Governance & Finance 21st July 2026
Ratified at Full Council 29th July 2026
Review 2027