Sefton Council

Sending / Discussing Personal Information Policy

June 2024

Summary Sheet

Document Information

Protective marking (Official /Official-Sensitive-Personal/Official-Sensitive-Commercial/Official-Sensitive-Confidential)	Official
Ref	IG Procedure 6.0
Document purpose	Council obligations under Data Protection Act in relation to sending / discussing personal data via fax, e-mail, phone or post.
Document status (Draft / Active)	Active
Partners (If applicable)	N/A
Date document came into force	1/11/2014
Date of next review	June 2026
Owner (Service Area)	Sefton Council – Information Governance, Strategic Support
Location of original (Owner job title / contact details)	Data Protection Officer – as above.
Authorised by (Committee/Cabinet)	Information Management Group November 2014 Audit & Governance Committee June 2015

Document History

Version	Date	Author	Notes on revisions
1.0	November 2014	Ben Heal DPO who revised document purchased from Act Now IG consultancy.	On ICO advice to be taken to full Cabinet for ratification.
2.0	December 2020	Catherine Larkin Mark Quillan Steve Lawson	Reviewed following data incident
3.0	June 2024	Catherine Larkin	Inclusion of information about discussions within shared office spaces

Contents

1 Providing Personal Information Safely by Post 4
1.1 Introduction 4
1.2 Key Actions 4
2 Providing Personal Information Safely Over the Telephone 5
2.1 Introduction 5
2.2 When someone calls you asking for information 5
2.3 When you call someone 5
2.4 When someone calls to provide you with information 6
2.5 In-coming communications - process to be followed when entering data into systems 6
3 Discussions in the office 6

1 Providing Personal Information Safely by Post

1.1 Introduction

When sending out paper documents containing service user or other personal data, you must ensure that the documents are secure and properly addressed. You are responsible for ensuring that they are sent to the right people, safely packaged, and that they can safely be returned to you if not successfully delivered.

This is not just good office practice – accuracy of personal information and keeping it secure are key principles of data protection. This includes appropriate security of the personal data and protection against unauthorised or unlawful processing, accidental loss, destruction or damage, using appropriate technical or organisational measures.

Many organisations have been subject to enforcement action for not observing sensible procedures when posting personal data. It is just as important to send information securely internally as well as externally.

1.2 Key Actions

Ensure that the destination you are sending documents to is still in the same place – especially if the recipient is outside of the Council.

Check the address and send documents to a named person if at all possible, and not to a department or team. In all cases, do not address letters to an organisation without at least identifying the team.

Put a covering letter with the information – DO NOT put records or data into an envelope by themselves.

Seal the envelope securely and mark it **Private and Confidential on the front and back of the envelope.**

Send any personal or other sensitive information by special delivery and keep the tracking information.

All post which leaves a Council building for posting externally should have the return address stamped on the front of the envelope. This will allow a wrongly delivered envelope to be returned without having to be opened.

The Council, as the data controller that chooses to use a delivery service to transfer personal data, is the party responsible for the data. If a delivery service loses a letter or a parcel containing highly sensitive personal data, it is the data controller that sent the data that will be responsible for the loss. It was the data controller that chose to use the delivery service. If it was vital that the personal data was delivered securely, the data controller should have used secure delivery rather than an ordinary postal service.

2 Providing Personal Information Safely Over the Telephone

2.1 Introduction

All staff need to keep personal information about individuals secure and private at all times. Individuals are entitled to expect that their privacy and confidentiality is respected, and that their data are always treated with care and appropriate security.

For both confidentiality and legal reasons, it is vital that care is taken when providing information over the phone.

Using the phone carries a number of risks:

- Information may be transcribed incorrectly
- You cannot always be certain who you are dealing with
- You may be overheard

You must ensure when discussing individuals and/or their families that your conversation cannot be overheard by colleagues outside of your team. It is critical that we maintain the trust that our service users and customers place in us.

2.2 When someone calls you asking for information

Establish who you are speaking to before you disclose any information. Identify the person clearly, check who they work for and what they want.

If a person demands information, check their entitlement to receive that information.

Unless you are certain that the person is who they say they are, get their switchboard number (not their direct number) and ring them back. Check the switchboard number from their website, not from them.

If in doubt, ask them to put their request in writing. Any request for access to the personal data of a third party must be made in writing. If you are unsure about whether or not to disclose the information, check with your Line Manager, Information Asset Owner or the Council's Data Protection Officer.

2.3 When you call someone

If you are calling to provide information, be certain that the phone is the best way to provide information. In many cases it is better to provide it in an email (which allows a specific record of the information to be retained). If the information is personal or sensitive, you must use a secure form of e-mail, such as Egress.

Ensure you speak to the person who needs the information – never leave personal or sensitive data in a message.

2.4 When someone calls to provide you with information

Ensure you record information accurately – check the information with the person providing it. Do you have the spelling, numbers and details right? It is very easy to make a mistake when noting down telephone numbers and email addresses. Read the information back to the caller to double-check.

2.5 In-coming communications - process to be followed when entering data into systems

It is vital to ensure that all incoming communications received by the Council, whether received face to face, by phone, email or postal correspondence, are accurately matched with the data subject they concern before being entered into relevant Council systems for processing. Inaccuracies and mistaken identity at this stage create an inherent risk of serious data security breaches when subsequently processing and responding to communications which have been linked to the wrong data.

Officers with responsibility for entering data into systems, whether receiving information by phone call, face-to-face, email or in the post, must identify and reject items which fail to meet the two-identifier standard at the point of receipt.

Where possible, further suitable and relevant data must be requested before the communication can be accepted and processed.

Face-to-face customers must be asked for a minimum of two items of relevant documentary identification or identifying information.

Customers on the phone must be asked for a minimum of two items of identifying information.

Telephone messages, emails, postal communications etc. must be checked for a minimum of two items of identifying information before being imported into systems or processed in any other way. Where identifying information is found to be insufficient, a reply, sent via the same channel or via contact details provided within the original communication, should be issued requesting such additional identifying information as is relevant and appropriate.

If it is not possible to respond and request further identifying information, e.g. a written note containing no contact details, then the communication cannot proceed any further and must be discarded.

3 Discussions in the office

The Council needs the personal data of its employees, citizens of the Borough and customers to be able to function properly and undertake its tasks and obligations. We are trusted to look after this information and every employee has a responsibility

to comply with the UK data privacy laws. This means keeping personal information about individuals secure and private at all times.

Individuals are entitled to expect that their privacy and confidentiality is respected, and that their data are always treated with care and appropriate security.

Therefore, for both confidentiality and legal reasons, it is vital that care is taken when having professional discussions in the office.

You must ensure when discussing individuals and/or their families that your conversation cannot be overheard by colleagues who have no right to hear the content. It is critical that we maintain the trust that our service users and customers place in us.

This could be a breach of data protection legislation if you reveal personal data about an identifiable, living individual.

Wherever possible, book a meeting room in a Council building or have the conversation via MS Teams at home, ensuring you cannot be overheard by anyone who lives with you.

When this is not possible and the conversation has to take place in an open office which may be overheard by colleagues outside of your team, be mindful of how loud your voice may be, what you are saying and who is in the near vicinity and may be able to hear you.