

Personal data security: how to prevent some common personal data breaches in the Local Government sector

1. How to disclose information safely

Check documents, including spreadsheets, for hidden personal information and remove or redact it, where appropriate. This will minimise the risk of an accidental breach of personal information when disclosing documents online or sending them to the public. See our guidance on [How to disclose information safely](#) for more information.

2. Always double check

Double check that you are providing the right information to the right people. This applies whether you are providing personal data electronically, by post or in person. Send regular reminders to staff about the importance of always double checking and emphasise the significance of verifying recipients.

3. Send documents securely

Consider password protecting any documents sent electronically, especially documents that contain sensitive information. This can help to keep information secure and prevent it from being accessed by an unauthorised individual. In addition, consider providing the recipient with the password via an alternative method, such as telling them over the phone or sending it via text.

4. Clearly mark any data handling requests for all staff to see

Some individuals have specific requests about how their data is handled. There may also be safeguarding reasons that mean you need to handle a record with care. You should have strong mechanisms in place to clearly mark alerts on your systems in cases like this. This should be transferred across all systems that hold these records. Clear processes should be in place for staff to follow. All staff handling this information should be aware of the checks they need to make before disclosing information.

5. Take time to review any redacted documents

Organisations should have robust redaction procedures in place to ensure that no third-party information is inadvertently revealed. Double-checking before disclosure helps prevent accidental breaches. You should also ensure that appropriate redaction software is used to reduce the risk of personal data being shared with the wrong person.

6. Keep your records up to date

Periodically review your records to ensure that they are kept up to date. You should have a procedure in place to verify records you hold are current and accurate. This could prevent you accidentally disclosing information by using someone's previous contact details.

7. Make sure your systems are working correctly

Whether you are sending out a large amount of letters for a new initiative using a mail merge or using software to redact a document, you should be confident that the systems you are using are working correctly. Check your systems regularly so that any flaws or errors can be identified and fixed before a breach happens.

8. Have clear policies and guidelines about staff responsibilities.

Ensure you are confident in the clarity and robustness of any written policies or guidelines. These should make the requirements clear to staff about handling personal data on behalf of the organisation. These policies and guidelines should emphasise the importance of confidentiality and clarify that employees should not disclose information without authorisation or a business need. They should also outline what information can and cannot be accessed as part of their role.

9. Ensure the safe disclosure of information when responding to Freedom of Information Act (FOIA) requests

Reduce the risk of disclosing personal information accidentally by ending the use of original source excel spreadsheets when publicly responding to FOIA requests. You should avoid using spreadsheets with hundreds or thousands of rows and invest in data management systems which support data integrity. Staff who use common data software and are involved in disclosing information should receive regular training. See our guidance on [How to disclose information safely](#) and our [checklist for public authorities to use for the safe and appropriate disclosure of information](#).