

Data Protection Impact Assessment (DPIA)

Project/Procedure/Contract Title: Postal Services - Hybrid mail Solution

Lead Officer: Helen Bishop

DPIA Completion Date: 19/05/2025

DPIA Completed by: Tim Martin

Relevant Documents: [Please include a hyperlink here]

Approvals: This Document must be approved by the Data Protection Team.

“Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data”

General Data Protection Regulation Article 35 (1)

Data Protection Impact Assessment (DPIA)

1 Background

The Council produces in the region of 300,000 bills and statements for Council Tax, Business Rates, Rents, Garages, Leaseholders and Benefits per annum. In addition to this sum, the Council produces the Tenants in Touch newsletter which is circulated to circa 8,000 tenants on a quarterly basis; some 30,000+ items per annum. There is an unknown volume of other materials which need to be produced and posted. These are delivered, through traditional means, via the Council's Corporate Support team (postal services).

In 2021, a contract for a hybrid print and post solution was awarded to PSL Print Management Ltd. This contract managed the aforementioned documents and enabled the distribution of ad hoc mail.

The hybrid print and post contract expires 30th November 2025, and a new contract is being tendered.

A market engagement exercise was completed in April 2025 and has informed the development of a tender specification for a future, replacement solution.

2 Project/procedure/Contract Benefits

This project seeks to tender for a replacement contract for the equivalent services. In addition, any tender exercise will seek to take advantage of digital distribution that will support the Council's agenda for channel shift and cost reduction.

The project produced a business case for the sourcing and letting of a contract for the printing and onward distribution of key documentation to tenants and residents through a hybrid mail provider.

Contracting with a hybrid mail provider releases the Council from having to print, prepare and stuff envelopes, and then directly post the printed matter. Using a hybrid mail provider reduces the costs of Council resource, print and post machinery, and consumables.

The Council has an existing contract, for outbound, hybrid postal services, with PSL Print Management Ltd (PSL). The contract was awarded in 2020 and is due to conclude on the 31st of October 2025.

Where paper correspondence is unable to be delivered via the PSL contract, the Council maintains a reduced, but traditional postal service for outbound mail. Reasons for this continued service are where the supplier may have a system outage or where an urgent postal despatch is required and the time to transmit, prepare and deliver via the contract would take too long.

The allocated budget for post and print services (for 2025/2026) is £216,040 of which a budget of £63,440 specifically relates to contract (bulk) printing.

Consideration has been given to ascertain if the Council can bring this contract in-house to deliver the same standard of operation, and a reduced cost as currently paid within the PSL contract. This is not a viable option as to do so would require investment in both new resource and machinery infrastructure to service and deliver the required volumes of post on a daily, quarterly, and annual basis. Additionally, the Council is unable to provide the Royal Mail with post of a 'sorted' status, and for this reason, will continue to attract a higher per item price.

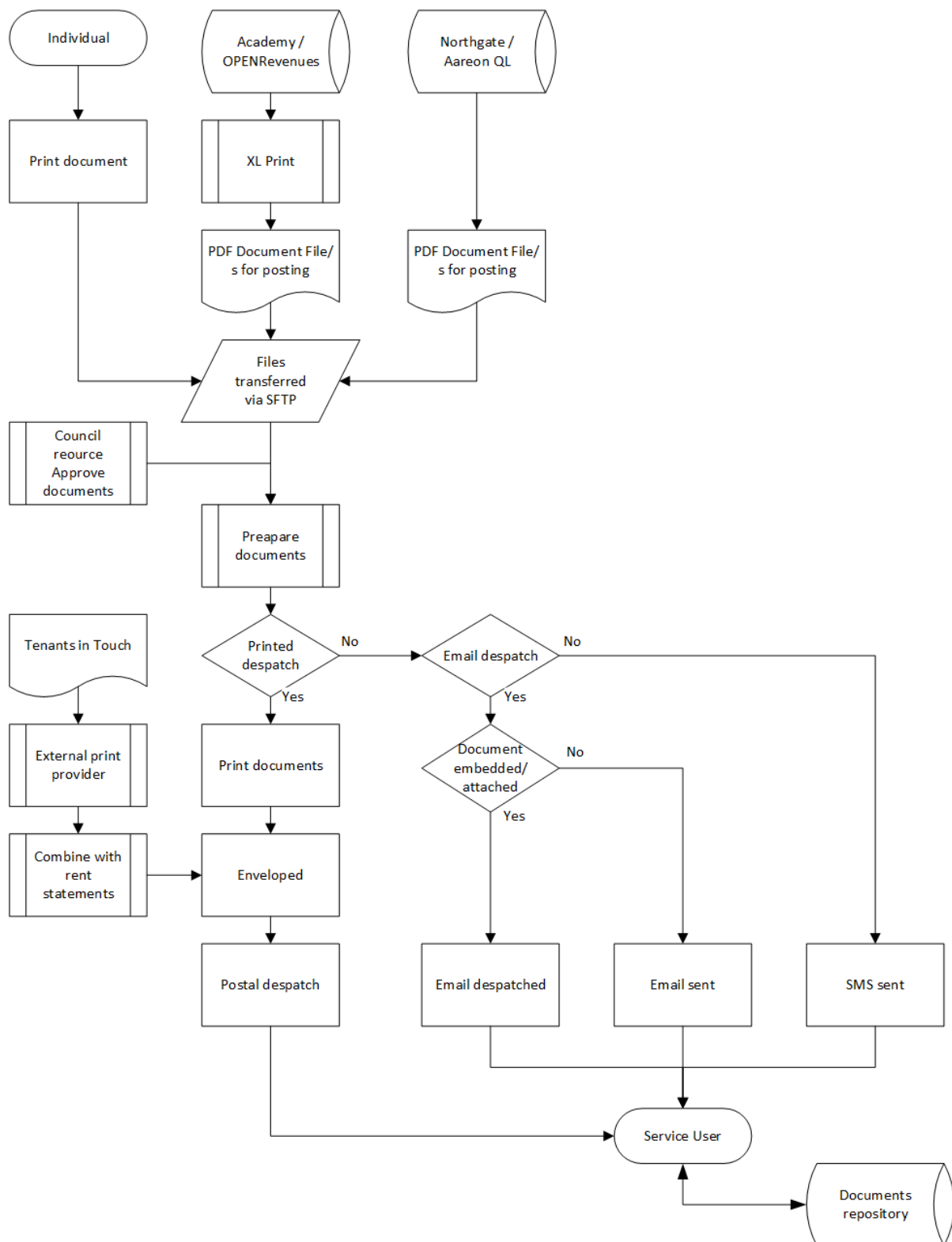
Letting a contract of this nature will ensure the Council distributes key documents to its tenants and residents whilst internally, keeping costs at a minimum.

3 Data Flow

For the current contract, the diagram below shows how relevant information is extracted from our key systems and formatted as PDF versions of the documents for printing and despatching.

The new contract will enable additional functionality, including the ability for individuals to submit information for despatch. Alternative methods include the emailing of documents and electronic notification (email and SMS) which enables a service user to access a secure document repository from which they will be able to retrieve their document/s.

The following image will be reviewed once the project progresses with a preferred supplier and further information is understood on the process.



4 Data collected for Project/Procedure/Contract

“Personal data means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental,

economic, cultural or social identity of that natural person” (General Data Protection Regulation Article 4 (1))

Please select from the below options which types of Personally Identifiable Information (PII) you will be collecting during the project/procedure/contract. (Click the box to select)

The project will not specifically collect data, however, the project will provide a postal function that will be available to Service Areas and their Teams and individual staff members. The project will enable the transmission of data recorded or extracted from our systems and ad hoc communication. Given this position, all bar one of items below have been checked.

- ☒ Name
- ☒ Contact Details (i.e phone number, email address)
- ☒ Account/Membership number
- ☒ Date of Birth
- ☒ Location information (i.e. Postal Addresses, IP Addresses)
- ☒ *Sex/Gender/Sexual Orientation
- ☒ *Race/Ethnic origin
- ☒ *Health information (i.e. Disabilities)
- ☒ *Financial information (i.e. Bank account details, income)
- ☒ *Political Affiliations/Trade union membership
- ☐ *Biometric Data (i.e. fingerprint, facial recognition)
- ☒ *Criminal Convictions or Offences
- ☐ Other

Article 5 under GDPR states that “Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”

*For each box ticked please explain why this category of PII is **essential** to the project/procedure/contract.*

Information captured is determined through the operational processes related to both processes across the Council where we write to the service user. This project does not determine any of the information, it is simply taking extracted information directly (or via XL Print) in Microsoft Word or PDF format and transferring it to a hybrid mail provider for printing and onward despatch.

Categories with the (*) are deemed as ‘special personal data’ under GDPR and require increased security (Article 9). If collecting any of this PII please explain below what additional measures you have put in place to secure this data.

Information is provided as Microsoft Word (converted to PDF format) or provided in PDF format. The files are transmitted to the hybrid mail provider via a secure file transfer protocol (sftp).

5 Lawfulness of processing

Please select from the below options which basis you will be using to collect the Personally Identifiable Information (PII) during the project/procedure/contract. (Click the box to select)

- ☐ Consent gained from Data Subject to process their PII*
- ☒ Processing the PII is essential to fulfil a Contract with the Data Subject
- ☐ There is a Legal Obligation to process the PII (please explain below)
- ☐ Processing the PII will protect the vital interests of a Data Subject (please explain below)
- ☐ Processing the PII is in the public interest (please explain below)

**If you are gathering and processing PII on the basis of consent please explain where evidence of this consent is stored?*

Consent for the processing of PII Data lies with those responsible for communicating with service users.

This project is concerned with the transmittal of documents to a hybrid mail provider for printing and/or onward distribution to service users.

**Do you have a mechanism to stop processing an individual's PII if they withdraw their consent?*

This project has no ability to stop processing an individual's PII data if they withdraw their consent. This project has no control over the collection of PII data.

If you are gathering and processing PII on the basis of vital or public interests, or as a legal obligation please explain this in more detail.

This project has no influence over the gathering and processing of an individual's PII data.

N.B. Regardless of the basis for processing PII the Data Subject must be informed of what data you are processing, for what purpose, and under what basis. For more information please refer to GDPR Article 6 & 12

6 GDPR Compliance – Questions to consider

1. *Will the Councils privacy notices need to be amended to reflect this new project/procedure/contract?*

NO. This project is seeking to award a contract (to a new or existing provider) for an existing arrangement.

2. *How will you monitor whether the information you hold is accurate?*

Data is extracted from the Council's line of business applications. Once transmitted to the hybrid mail provider, there is a process whereby the Council reviews and confirms the data. Once confirmed, the data is committed to print.

It should be noted, if an ad hoc hybrid mail solution is sought, some documents will be produced locally, by Council Officers and Staff. The content of the documents is at the discretion of the individual

3. *Do you have the capability to amend or delete information if necessary?*

Yes. Files produced via line-of-business systems are transferred to the hybrid mail provider. Once prepared, Council Officers and Staff are asked to confirm the contents prior to printing. If errors are identified, they can be corrected.

For Ad hoc files, the content is produced by individuals, but the same principle is applied.

4. *Do you have a mandated retention period for this data? If so what is it?*

Internally, data is retained in line-of-business systems and by Service Areas, Teams and individual in accordance with the Data Retention Policy (to be adopted).

Market engagement has indicated suppliers retain information for circa 60 days, however this will be fully established through the tender process.

5. *What are the means of communicating with the data subjects?*

This project enables the print and distribution of key documents to service users. Suppliers also have the ability to provide information via email and SMS. The tender process will examine suppliers ability to support the Council in seeking opt-in/opt-out confirmation for electronic means of communication..

6. *Is the scope or purpose for processing information collected likely to change in the future? (i.e. the information required to set up a new system may differ from information required to continue business as usual)*

Existing line of business systems are being replaced. Data extracted will need to be formatted in new templates for onward distribution.

An ad hoc document, hybrid mail solution will be sought.

7. *Are any of the data subjects under 13? If so do you have a mechanism for regaining consent or informing them of the purposes for processing their data once they turn 13?*

There are no data subjects under the age of subjects under the age of 13.

8. *Will you be transferring data outside of the EU? If so, where?*

The secure ftp site location will be taken into consideration in the tender assessment and award process. Data located in the European Union has been included as a requirement in the specification.

9. *Where a third party is processing the PII have you confirmed they are GDPR compliant? Do you have a contract in place, explaining your expectations regarding the security of your data?*

GDPR compliance forms part of the requirements specification documentation. GDPR compliance will be taken into consideration in the tender assessment and award process.

7 Risks & Mitigating Actions

“Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk” (General Data Protection Regulation Article 31 (1))

Data Breach: A data breach constitutes any unauthorised loss, destruction, alteration, disclosure of, or access to, personal data, whether accidental or malicious.

Risk	Impact	Mitigating Action	Owner
<i>What is the scenario in which data might be lost, unlawfully accessed etc.</i>	<i>When deciding impact take into consideration the number of individuals involved and the sensitivity of the data.</i>	<i>Any actions taken to reduce the likelihood of this risk occurring.</i>	<i>Who is responsible for completing the mitigating action (N.B this is not who is accountable for ensuring that it is done)</i>
Files of tenant and resident financial information are intercepted	Tenant and resident financial information is obtained	Files are transferred via a secure ftp site for the hybrid mail provider to collect.	E.g. IT – for encryption software Managers - for updating procedure Officers – for following new procedure
Files of tenant and resident information are passed on to a 3 rd Party	Tenant and resident information is exposed/lost	Data security/data protection agreement must be in place with the hybrid mail provider	Contract Owner
Breach of Data Protection occurs at the hybrid mail provider	PII and Special Category Data is lost	The Council are informed immediately. Breach reported to Regulator. Investigate and attempt to recover data	Process Owner within the Council and hybrid mail provider
Cyber-attack on data in transit	PII and Special Category Data is lost	Provider to have secure encryption in place for transfer of data	Contract owner/Supplier

Common risks to consider:

- Risk that the security of the data is compromised
- Risk of unauthorised access to the data whilst held by the Council
- Risk that the individuals would object to the processing when informed
- Risk that the accuracy of the data is not maintained
- Risk that personal data is retained for longer than is necessary.

For all mitigating actions identified, have you assigned a budget for fulfilling them?

- ☐ Yes
- ☐ Not Yet
- ☒ Budget not required.

The risks will be part of the tender assessment and award recommendation process.

8 Sign Off

The Council's Data Protection Team must be consulted on the completion of the Data Protection Impact Assessment, and approval must be gathered before the project or contract is signed off.

Project Manager sign off

Project Manager Name:	Signature:	Date:

Data Protection Team Sign off

Data Protection Officer Name:	Signature:	Date:

9 Appendices

This page is intentionally left blank