www.oxford.gov.uk

OXFORD CITY COUNCIL

Appendix 3

Data Protection Impact Assessment (DPIA)

Project/Procedure/Contract Title:	[HR and Payroll System Procurement]
Lead Officer:	[Steph Nichols]
DPIA Completion Date:	22 December 2025
DPIA Completed by:	[Steph Nichols and Becky Willis]
Relevant Documents:	[Project Control Document V0.1 July 20252.docx]
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

Explain the context of the project/procedure/contract; provide a brief description and business reasons for undertaking the project/procedure/contract.

This project aims to support the timely procurement of a new HR and Payroll management system to replace the current platform (iTrent) provided by Midland HR. The existing contract, which began in 2018, will reach its maximum permitted term in March 2028 after all extensions are exercised. This timeline ensures continuity while other major corporate systems are implemented and avoids disruption to critical HR and payroll functions.

Re-procurement is required to meet statutory obligations and procurement rules. The final extension provides sufficient time for mobilisation and a phased transition, including parallel running and contingency measures, to safeguard business continuity. The current system supports approximately 1,500 employees across the Council and Oxford Direct Services Ltd, delivering essential HR lifecycle processes, payroll, recruitment, absence management, and statutory compliance.

A modern solution is needed to address the limitations of the existing system, align with the Council's digital transformation objectives, and improve functionality, user experience, and integration with other corporate systems. This project will enhance operational efficiency, ensure compliance, and support strategic goals during a period of organisational change.

2 Project/procedure/Contract Benefits

Briefly explain the benefits of the project/procedure/contract to the Council, the Data Subject and other parties.

The expected benefits of procuring and implementing the new system are:

- Increased efficiency in HR and Payroll operations
- Enhanced employee experience through improved self-service functionality
- Accurate and timely payroll processing
- Advanced reporting and analytics to support data driven decision-making
- Seamless integration with other Council systems and platforms

3 Data Flow

Using a flow diagram, please show how data will be collected, shared, and destroyed through the new project, procedure, contract or system.

High-Level Summary of Likely Data Flow

- Personal data will be collected from employees and contractors via secure onboarding forms and self-service portals. This data will then be processed by HR and Payroll teams for employment and payment purposes, stored securely within the chosen HR/Payroll system, and shared only with authorised third parties such as HMRC, pension providers, and statutory bodies. Data will be retained in line with the People Team's retention schedules and securely deleted when no longer required.

- **Note:** A detailed data flow diagram will be added once the system has been procured and the technical architecture is confirmed.

The Council will work with the chosen supplier to map and document the full data flow once the system is selected.

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)

- ☒ 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 <u>limited to what is necessary</u> in relation to the purposes for which they are processed"
*For each box ticked please explain why this category of PII is <u>**essential**</u> to the project/procedure/contract.*

- Name – essential for identifying the employee or contractor.
- Contact Details – required for communication regarding employment matters.
- Account/Membership number – used for internal HR/payroll system identification.
- Date of Birth – necessary for verifying identity and calculating age-related entitlements.
- Location information – required for payroll tax purposes and emergency contact.
- *Sex/Gender/Sexual Orientation – collected for equal opportunities monitoring and reporting (provision of this data is optional)
- *Race/Ethnic origin – collected for diversity and inclusion reporting (provision of this information is optional)
- *Health information – necessary for managing absences, reasonable adjustments, and statutory obligations (provision of this data is optional)
- *Financial information – required for salary payments, pensions, and benefits.
- *Political Affiliations/Trade union membership – processed where relevant to deductions or representation.
- *Criminal Convictions or Offences – processed where required for safeguarding or legal compliance.
- Other – employment history, qualifications, and performance data for HR management.

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.*

- All special category data will be encrypted in transit and at rest, in line with ICO and NCSC recommendations.
- Access will be strictly limited to authorised employees only, based on role-based permissions. This includes People Team employees for system maintenance. Line managers will only access data necessary for their role (e.g., absence management), documented in an access matrix.
- Multi-Factor Authentication (MFA) will be enforced for all users with access to special category data, using phishing-resistant methods where possible.
- Comprehensive audit logs are maintained to track access and changes.
- Data will be stored in secure UK-based data centres certified to ISO 27001 and Cyber Essentials Plus. Supplier contracts will include GDPR compliance obligations and security standards.
- Regular penetration testing and vulnerability assessments will be conducted to validate security controls and maintain compliance with Article 32 of GDPR.

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?

Evidence of consent will be captured electronically within the system during onboarding or when optional data (e.g., diversity monitoring) is provided. The system will store a timestamped record of consent linked to the employee profile. These records will be:

- Encrypted at rest and protected by role-based access controls.
- Auditable, with logs showing when and by whom consent was given or withdrawn.
- Retained in line with the Council's data retention schedule for HR records.

In exceptional circumstances where digital consent is not practical, paper forms may be used. These will be scanned and uploaded to the secure HR system and destroyed once digitised to maintain GDPR compliance.

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

The HR and Payroll system will include functionality to record and act on consent withdrawal. When an individual withdraws consent for optional data processing (e.g., diversity monitoring), the system will:

- Immediately flag the record and remove the relevant data fields from active use.
- Trigger an automated workflow to delete or anonymise the data in line with retention policy.
- Update audit logs to record the withdrawal event, including timestamp and user details.
- Notify the relevant responsible person or team to confirm compliance and ensure any manual follow-up actions are completed.

Employees will be able to withdraw consent via self-service or by contacting the People Team. Clear instructions will be provided in privacy notices and onboarding materials.

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.

Certain categories of personal data will be processed under the following lawful bases:

- **Legal Obligation**
  Processing is required to comply with statutory duties, including:
  - Payroll and tax reporting to HMRC.
  - Pension contributions and statutory deductions.
  - Employment law requirements such as right-to-work checks and safeguarding obligations.

  These activities are mandated by UK employment and tax legislation and cannot be carried out without processing personal data.

- **Public Interest**
  Processing supports functions carried out in the public interest or in the exercise of official authority vested in the Council, such as:
  - Workforce monitoring and equalities reporting under the Equality Act 2010.
  - Compliance with transparency and accountability requirements for public sector employment.

- **Vital Interests**
  In rare cases, processing may be necessary to protect the vital interests of an individual, for example:
  - Emergency contact details used in urgent health or safety situations.
  - Health information processed to ensure reasonable adjustments or respond to medical emergencies.

All such processing will be documented, limited to what is necessary, and carried out in accordance with GDPR Articles 6 and 9.

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

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

Yes. Privacy notices will be updated before go-live to include details of the new system, lawful bases for processing, and data subject rights. Updates will be published on the Council's website and communicated to staff via internal channels.

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

Data accuracy will be maintained through regular audits, employee self-service functionality, and automated validation checks during data entry. Discrepancies will trigger alerts for correction.

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

Yes. Authorised users will have role-based permissions to amend or delete records in line with Council policy and retention schedules. All changes will be logged for audit purposes.

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

Data will be retained in accordance with the Council's HR retention schedule (Retention Schedule V2.2.docx). The system will support automated retention rules and secure deletion.

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

Communication will be via letter to home address and secure channels including email, employee self-service portal, and internal People Team communications on the intranet. Privacy notices and consent options will be clearly accessible.

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)*

Yes. Any changes to scope or purpose will trigger a review of the DPIA and updates to privacy notices. Data subjects will be informed where changes affect their rights or data use.

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?*

No. The system does not process data for individuals under 13. If this changes, mechanisms for parental consent and age verification will be implemented.

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

No data will be transferred outside the UK/EU. Supplier contracts will include restrictions on international transfers and compliance with UK GDPR.

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?*

Yes. All third-party processors will be required to sign Data Processing Agreements (DPAs) and provide evidence of GDPR compliance, including security certifications (e.g., ISO 27001).

10. Does your project involve the use of Artificial Intelligence (AI)?

No, the system does not currently involve the use of AI or automated decision making. If this changes during the project and procurement process, we will assess data protection impact.

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, discloser of, or access to, personal data, whether accidental or malicious.

Risk	Impact	Mitigating Action	Owner
What is the scenario in which data might be lost, unlawfully accessed etc.	*When deciding impact take into consideration the number of individuals involved and the sensitivity of the data.*	*Any actions taken to reduce the likelihood of this risk occurring.*	*Who is responsible for completing the mitigating action (N.B this is not who is accountable for ensuring that it is done)*
E.g. Emails containing details of criminal convictions of tenants are intercepted	E.g. The email contains sensitive personal data about [a few/many] individuals therefore the impact is high. *If the data is sensitive personal data the impact will always be high regardless of number of individuals affected (Unless security is high enough that data is unintelligible to anyone without approved access).	E.g. IT are to install encryption software onto Officers devices and Officers are now to encrypt these emails as part of the procedure.	E.g. IT – for encryption software Managers - for updating procedure Officers – for following new procedure
Security of the data is compromised during supplier handling	The system contains sensitive employee and payroll information, therefore the impact is high if PII is accessed.	Require GDPR-compliant contracts, ISO 27001 certification, UK-based hosting Specification requires comprehensive audit trails for all changes and data exchanges, including tamper-proof logs retained for 12 months. Specification requires documented and tested disaster recovery plan. Specification requires regular system updates	People Team - for overseeing specification and implementation Legal Team – for ensuring Terms and Conditions of contract cover adequate GDPR and ISO compliance. Software suppliers (incumbent and new suppliers) – for data encryption, disaster recovery plan and security patches.

		and security patches.	
Unauthorised access to HR/Payroll data	High – risk of identity theft or misuse The system contains sensitive employee and payroll information, therefore the impact is high if PII is accessed.	Access to data will be limited at the individual, team or service level depending on user need. Each user will have a unique user ID and password. Multi-Factor Authentication (MFA) will be used. Data will be retained for 7 years after employment has ended. User access will be amended if there is a change of job role. Audit logs will be used. Regular training on data protection and security protocols will be provided for all staff, and role-specific training will be provided for HR and payroll staff.	The People Team will manage access and data retention. The ICT Team will maintain MFA/ single sign-on and oversee cyber security measures. Managers are responsible for recording roles changes accurately. Individual users are responsible for keeping passwords and user IDs confidential.
Individuals object to the processing when informed	Low – reputational risk	Update privacy notices, provide clear communication and opt-out mechanisms for optional data.	People Team/Information Governance The People Team will update privacy notices, with advice from Information Governance
Accuracy of data is not maintained	Data protection law will be breached and the organisation may be fined. Payroll errors are possible. Medium impact.	Enable employee self-service updates and conduct regular data audits. Provide training for managers to ensure they understand their responsibilities and how to update and check details in the system.	Managers are responsible for ensuring changes in employee details and roles are recorded accurately. The People Team is responsible for data audits and for oversight of processes for updating the system.
Personal data is retained beyond statutory limits	Medium – GDPR non-compliance Data protection law will be breached and the organisation may be fined.	Ensure system can apply automated retention rules and that reporting functionality can be used to support regular data audits. Conduct periodic data purges.	The People Team will be responsible for retention rules and processes and data audits.
Security of data is compromised during data	The system contains sensitive employee and	Manage data migration in compliance with GDPR and robust cyber security	People Team supported by ICT Team - for overseeing specification

migration	payroll information, therefore the impact is high if PII is accessed.	standards. Use encrypted transfer protocols, secure staging environments, and supplier compliance checks	and implementation People Team supported by Procurement Team - for supplier compliance checks. Legal Team – for ensuring Terms and Conditions of contract cover adequate GDPR and ISO compliance. Software suppliers (incumbent and new suppliers) – for data encryption and staging environments.

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.

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:** 22/12/25
Stephanie Nichols		

Data Protection Team Sign off

Data Protection Officer Name:	**Signature:**	**Date:**