Privacy Impact Assessment

Recruitment System Replacement Project

DERBYSHIRE County Council

July 2017

Version History			
Version	**Date**	**Detail**	**Author**
1.0	07/07/17	1st Draft for Comment	[redacted]
2.0	14/07/17	Completed following comment from Audit and ICT	

Section 1
Step one: Identify the need for a PIA

- *Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties.*

- *You may find it helpful to link to other relevant documents related to the project, for example a project proposal.*

- *Also summarise why the need for a PIA was identified (this can draw on your answers to the screening questions).*

It is essential for the council to have a replacement on-line recruitment system to ensure that it can continue to attract applicants both internally and externally and support the internal jobs market, redeployments and organisational restructures. The current system has been provided by Abacus e-media since 2003 and is due to expire on 31 July 2017, but includes the option for the Council to extend on a month by month basis up until 31 December 2017.

Currently, of the 3,700 posts advertised a year, 84% of the 30,000 job applications made to the council each year are online. Without an e-recruitment system the council would have to manually process many recruitment activities, including providing applicants with requests for information about vacancies, applications forms, interview notifications, and management information.

10 supplier responses to the Pre-Qualification Questionnaire were assessed as compliant by the evaluation team, which consisted of representatives from HR and ICT services, and included robust security related questions. The six highest scoring companies were invited to tender and of the five submissions, Abacus e-media achieved the highest total score, after evaluation, clarification and due diligence. Cabinet of 25 April 2017 approved the award of a contract for the supply and support of a replacement recruitment system for a period of five years, with an option to extend on an annual basis for a five further years.

The benefits of the system to the council and stakeholders include:

- integration with SAP HR and payroll modules,
- a single entry process,
- a manager self-service element enabling managers to track the whole recruitment process,
- automation of ‘chasing’ pre-employment checks,
- improved access to vacancies for all potential applicants,
- the ability for applicants to track progress of their applications, and receive communications via email rather than letter,
- better management information.

As within the current recruitment system, the new system will hold information that individuals – both the public and employees – have provided about themselves because they are interested in applying for jobs within the council or with partners who advertise on the Council's jobsite. Current partners include six District Councils within Derbyshire, and the Peak District National Park. Some of the data is highly sensitive e.g. in relation to equalities monitoring groups and disability.

The information the individuals provide is used only when considering an individual for a vacancy within the council, in line with the Council's recruitment and selection procedures. Where requested by an individual, their contact details and personal preferences are used to enable the council to alert them to any potentially suitable job opportunities.

Taking into account:

- extensive personally identifiable data is held within the recruitment system,
- the sensitivity of some of the data held
- that the system is publicly accessible by a wide range of stakeholders
- the new recruit system will be externally hosted/Cloud based rather than internally hosted as currently.

Comprehensive steps have been taken throughout the project to identify and minimise the privacy risks of the new system and these are captured in the Privacy Impact Assessment.

See Business Case TP3677: Replacement e-Recruitment System for further detail.

Step two: Describe the information flows

- *You should describe the collection, use and deletion of personal data here and it may also be useful to refer to a flow diagram or another way of explaining data flows.*
- *You should also say how many individuals are likely to be affected by the project.*

Individuals affected by the new system will include:

- Recruiting Managers within Derbyshire County Council
- Schools and partner organisations using the system
- All applicants to jobs within the council – 30,000 applications were made in 2015/16 to 3,700 posts.
- Potential applicants for jobs within the council – 'registered users' who may request email alerts for specific vacancies.

Information collected during the recruitment process is retained in accordance with the Human Resources retention schedule.

Only information required at each stage of the recruitment and selection process as requested. The key flows of information are summarised below:

User Registration

The user provides basic information; Name, Address, Email address, to be used within the system to register them as a user, enable pre-population of future applications for posts, and allow email job alerts to be sent where requested.

Other information such as date of birth or telephone number can be provided but is not mandatory.

Application for a job

Potential applicant completes a standard application form including the following fields: Name, NI Number, Employer and work history, Qualifications and education, Suitability for the job statement, References, Any association with a councillor or employee, whether or not they have a criminal conviction/charge, any other information required to meet their needs during the recruitment process.

The equalities monitoring form collects data on:

Date of birth, Racial/ethnic origin, Disability, Gender, Religion/belief, Sexual orientation, how they found out about the job and if they are a current employee.

Sensitive personal data collected on the equalities monitoring form is not accessible to anyone except authorised users within the HR SSC who process the data to produce anonymised management information e.g. to meet equalities monitoring requirements. These are also protected fields within SAP.

To enable the Council to meet its commitments as a Disability Confident employer, the Recruiting manager will see 'Disability yes/no' against each candidate at the shortlisting stage. This will enable disabled candidates who meet the essential criteria to receive a guaranteed interview.

Recruiting Managers – access the application forms relevant to the vacancy they are advertising. The members of the interview panel also have access to the application forms. The equalities monitoring forms are detached/withheld by the HR SSC.

Non-shortlisted application forms are retained in line with HR Retention schedule.

Shortlisted forms are retained until interview/selection process is completed, and in line with the HR Retention schedule.

References and Occupational health recommendations are viewed by the Recruiting Manager before confirming a candidate's appointment to a role. References are only obtained before interview for certain roles to which specific Safer recruitment practices apply.

There are specific procedures around the handling of Criminal record disclosures, which are outside the system. The routine disclosure and barring service pre-employment checks are processed within a separate system.

Consultation requirements

- *Explain what practical steps you will take to ensure that you identify and address privacy risks.*
- *Who should be consulted internally and externally?*
- *How will you carry out the consultation? You should link this to the relevant stages of your project management process.*
- *You can use consultation at any stage of the PIA process*.

Stakeholders consulted and involved from the inception of the project, through the initial development of procurement specifications, through to the ongoing implementation include, ICT services, ICT Security Team, Procurement, Audit, HR and Legal Services.

The Security Team were consulted on the classification of the data and on the requirements to be included in the tender specification, and the areas of risk which should be fed into the risk register.

The Council's Information Governance Group have been consulted on the information security implications of the project.

As part of the Project Governance process, the Project Board consisting of the above stakeholders, have identified and monitored risks through the project risk register, including those relating to personal data held within the system.

Throughout the project key requirements have at every stage of procurement and implementation have been that the solution is technically robust, protects data integrity and holds data securely, and complies with the Council's existing standards, e.g. ISO 27001 and Data Protection act.

Step three: Identify the privacy and related risks

- Identify the key privacy risks and the associated compliance and corporate risks. Larger-scale PIAs might record this information on a more formal risk register.

- Annex three can be used to help you identify the DPA related compliance risks.

The project Risk Register developed and monitored through Project Board identifies risks associated with information security.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk
Data not retained securely – disclosure of information from system	Psychological distress of personal data being disclosed Financial loss due to impact on an individual job seeker's relationship with their current employer.	Non-compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation e.g. Employment equalities legislation	Reputational damage and loss of public trust Financial penalties Regulatory action Loss of employee trust
Individuals without the relevant permissions accessing data e.g. personal data provided on the application form, equalities monitoring data.	Psychological distress of personal data being disclosed	Non-compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation e.g. Employment equalities legislation	Reputational damage and loss of public trust Financial penalties Regulatory action Loss of employee trust
Collecting and holding excessive/irrelevan	Psychological distress through	Non compliance with ISO (or equivalent)	Resource implication of storing/processin

t for the purpose, or inaccurate information about individuals	perception of intrusion	Non-compliance with code of practice, DPA and other legislation e.g. Employment equalities legislation	g unnecessary data. Negative impact on organisational effectiveness and efficiency of processes.
Misuse of information – information used for other purposes that that specified e.g. equalities monitoring data including disability data being used at the selection stage	Reduces confidence in the application process Financial – as may impact on individual recruitment decisions when being considered for job	Discriminatio n Claims under equalities legislation Non-compliance with DPA, Code of practice and other legislation	Reputational damage and loss of public trust Financial penalties Regulatory action Loss of employee trust
Data retained for longer than is appropriate	Individual's information used for longer than appropriate or for new purposes, without individual's knowledge.	Non compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation e.g. Employment equalities legislation	Resource implication of storing/processin g data for longer than necessary. Negative impact on organisational effectiveness and efficiency of processes.
Consent to process personal data not collected at every necessary stage	Individuals do not understand what is happening to their data.	Non compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation.	Financial penalties Regulatory action Loss of employee and public trust

Data transferred outside EEA not adequately protected (?)	Psychological distress of personal data being disclosed	Non compliance with ISO (or equivalent) Non-compliance with code of practice, DPA and other legislation e.g. Employment equalities legislation	Financial penalties Regulatory action Loss of employee and public trust

Section 2
Step four: Identify privacy solutions

- *Describe the actions you could take to reduce the risks, and any future steps which would be necessary (eg the production of new guidance or future security testing for systems).*

General
The council has ISO27001:2013 certification and has established an information security management system in accordance with the requirements of ISO27001 and ISO27002 code of practice for information security controls.

The council requires the supplier to provide a level of information security assurance for Council and personal data compliant with current Data Protection Legislation and Information security best practice. The System requirements document TS14009 sections 2.1 'Technical Requirements' and 2.3 'Solution Security and Audit Requirements' set out the requirements which will be validated as part of the due diligence process.

Risk	**Solution(s)**	**Result:** is the risk eliminated, reduced, or accepted?	**Evaluation:** is the final impact on individuals after implementing each solution a justified, compliant and proportionate response to the aims of the project?
Data is not retained within the system securely.	Contract requires supplier to comply with Council security policies including Information Security Policy, Third Party Connection policy and Data Protection and Storage media	Eliminated	

	handling policy, and ISO27001 certificate or equivalent. Organisational information security policies and practices in place, and guidance for managers. Managers encouraged not to print out information e.g. application forms, where this is not required.		
Data on registered users retained for longer than required e.g. when no longer an 'active' user..	Archiving process being introduced to delete inactive accounts and associated data e.g. addresses, personal information. Registered users accounts to be 'refreshed; regularly to ensure they are still required.	Eliminated	
Data on people who have applied for vacancies retained for longer than required.	Automated deletion of records within system to comply with the data retention schedule requirements. Managers trained in information security. Revised recruitment and selection manager guidance to increase awareness of and compliance with HR retention schedule for electronic and manual records	Reduced – reliant on manager compliance with retention schedule.	

	held by the Recruiting manager.		
Consent to process information not rigorously obtained from individuals	All Privacy statements within the recruitment and selection process - both on the system and in paper processes - to be reviewed to ensure compliance.	Eliminated	
Unnecessary or irrelevant data held.	As part of system configuration and development it is ensured that data is only collected at the point it is needed, for at each stage of the recruitment workflow is collected and held, with clear justification as to why it is required.	Eliminated	
Inaccurate data held within the system.	Personal data primarily entered by the individuals themselves. System designed to be as user friendly to reduce inaccuracies. Effective training for managers and administrators to ensure the system is used in accordance with protocols and processes. System allows for corrections and amendments.	Reduced – human error when entering information not eliminated.	

Inappropriate access by individuals to sensitive data leading to misuse of data	Technical and administrative measures in place to prevent misuse of data e.g.. access controls based on user responsibility and job role. Effective access controls in place including authorisation levels, hidden fields for sensitive data. Requirements defined in contract with supplier, which will be audited/tested within the system, Council's stringent password policy complied with. The new system will enable the electronic delivery of recruitment related documents and information and therefore will reduce the security risks associated with paper documentation.	Eliminated	
Data stored in more places than necessary	Throughout project approach has been that data should only be stored where required e.g. Occupational health assessment outcomes held only in occupational health	Eliminated/Reduced – relies on all users of system including managers not duplicating information.	

	system, with necessary action for manager only, being held in Recruit system. Only minimum required information included e.g. in interface between SAP and Recruit system, and in data on organisational hierarchies within the system.		

Section 3
Step five: Sign off and record the PIA outcomes

- *Who has approved the privacy risks involved in the project? What solutions need to be implemented?*

Risk	Approved solution	Approved by
All the risks above have been identified by stakeholders as part of the development of the System requirement document, and reflected in the contract with the supplier and implementation plan.	The approved solutions above have either a) been identified by stakeholders as part of the development of the System requirement document, and reflected in the contract with the supplier or b) identified as part of implementation and incorporated into the implementation plan.	Project Board

Step six: Integrate the PIA outcomes back into the project plan

- *Who is responsible for integrating the PIA outcomes back into the project plan and updating any project management paperwork?*
- *Who is responsible for implementing the solutions that have been approved?*
- *Who is the contact for any privacy concerns that may arise in the future?*

Action to be taken	Date for completion of actions	Responsibility for action
Project Board to review PIA outcomes and ensure implementation plan reflects the approved solutions.	Expected to be by implementation of the system	Project Board

Contact point for future privacy concerns