Data Protection Impact Assessment (DPIA)

Why do I need to complete a DPIA?

This process is a mandated legal requirement of data protection legislation to ensure that privacy concerns have been considered and actioned to ensure the security and confidentiality of the personal identifiable information.

When do I need to complete a DPIA?

This document must be completed for any proposed, new or change in process, service, technology, or project which may or will be processing personal identifiable information. It must be completed before change, implementation, or procurement.

Who should complete a DPIA?

The DPIA should be initiated and completed by either the relevant Project Manager, Manager or Information Asset Owner/Administrator (IAO/IAA) Intranet | Information on the roles of SIRO, IAO, IAA, DPO and CG (york.gov.uk) in the area proposing the change.

It is advisable to include the following where appropriate:

- information governance team
- ICT & information security team
- web services team
- legal services
- procurement
- relevant stakeholders
- any data processors (including 3rd party suppliers)

Following completion of the DPIA, if it identifies a high risk and you cannot do anything to reduce it, we must consult with the ICO as set out in data protection legislation. You must not go ahead with the processing until this has been done and the ICO

has provided their decision or outcome Do we need to consult the ICO? | ICO You must contact information.governance@york.gov.uk who will lead on this with the ICO.

The DPIA must be approved and signed by the IAO/IAA or appropriate senior manager before the system goes live and/or the new or changes to processing, starts.

What Next?

If you have answered yes to any of the DPIA screening questions you will be required to complete the DPIA with as much detail as possible and return the completed from to information.governance@york.gov.uk

Further guidance on DPIAs can also be found on the Information Commissioner's website www.ico.gov.uk

What does 'large scale' mean?

The legislation does not contain a definition of large-scale processing, but to decide whether processing is on a large scale you should consider:

- the number of individuals concerned.
- the volume of information.
- the variety of information.
- the duration of the processing; and
- the geographical extent of the processing.

Examples of large-scale processing include:

- a hospital (but not an individual doctor) processing patient information.
- tracking individuals using a city's public transport system.
- an insurance company or bank processing customer information.
- a search engine processing data for behavioural advertising; or
- a telephone or internet service provider processing user information

Data Protection Impact Assessment (DPIA)

Reference Number (if applicable)	
Lead/contact name:	Nicola Grayson
Directorate:	City Development
Service Area:	Regeneration
Data controller details:	Regeneration team (Nicola Grayson)
Data processor details:	Regeneration team (Nicola Grayson)
Information Asset Owner: (All systems/assets must have an Information Asset Owner (IAO). Intranet | Information on the roles of SIRO, IAO, IAA, DPO and CG (york.gov.uk)	Katie Peeke-Vout, Head of Regeneration
Information Asset Administrator: (All systems / assets usually have an Information Asset Administrator (IAA) who reports the IAO as stated above. Intranet | Information on the roles of SIRO, IAO, IAA, DPO and CG (york.gov.uk)	Nicola Grayson
Customers and stakeholders: Please list all involved including both internal and external parties	Internal: • Communications team • Neighbourhood team • Highways • Public Realm • Regeneration • Transport

	External: • Council tenants • Private tenants/owners • Local businesses • Those travelling to/through the area • Students (who may also be residents)

Step 1 – Identify the need for a DPIA

Hints and tips to complete this section:

Refer to the completed DPIA screening questions

*It was identified that a DPIA would be needed ***.*

*The purposes of the proposed, new or change in process, service, technology, or project are ****this could be copies of extracts from or links to project docs, business cases etc****
*The above will realise several benefits including: *** e.g. what are the expected benefits for individuals/the council etc*

See customers and stakeholders above and/or describe when and how you will seek individuals' views – or the reasons it's not appropriate to do so and/or refer to the equalities impact assessment Intranet | Equalities and human rights (york.gov.uk)

If you need to describe "purposes" because there are no other documents, consider the below points

- *what do you want to achieve*
- *what is the intended effect and/or outcome for individuals, the council etc*
- *are there any unintended effects and/or outcomes for individuals, the council etc*

The South Walmgate programme aims to make transport and public realm improvements to the area adjacent to the former Willow House site that will be redeveloped into new housing. Additional projects may include a heritage trail, public art and communal gardening/planting schemes.

The DPIA screening identified that a DPIA would be needed as we:

- Want to keep people informed via an email mailing list
- May need to contact individuals if a project could directly affect an individual, such as construction work next to their home.

Approval of the Walmgate Masterplan will be taken to Executive for decision and so a DPIA is required.

Step 2 – Describe the information flow

Hints and tips to complete this section:

The collection, use and deletion of information should be described here.
It may be useful to use a flow diagram or another visual way or data map/flow/list to explain information flows.
If there will be any card payments taken as part of the processing, need to confirm if online and/or card machine and which "system" is used to process the payments taken

Names, emails and potentially addresses will be gathered as part of this project. This will be needed to communicate with residents, businesses and community organisations to invite them to events, canvass opinions/gather feedback and to communicate project updates and progress.

Provide details of personal, special category and criminal offence data being processed by checking all options that apply. Add any additional items and their description, in the 'other' option.

Personal data			
Name	☒	NHS Number	☐

Address	☒	NI Number	☐
Post Code	☒	IP Address	☐
Date of Birth/Age/Age group	☐	Photograph	☐
Telephone Number(s)	☒	Email Address	☒
Other: Please describe	☐		
Special Category Data			
Religion	☐	Ethnicity	☐
Health Information	☐	Trade Union Membership	☐
Political Opinions	☐	Sexual Orientation	☐
Biometric Data	☐	Other: Please describe e.g. Carer	☐
Criminal offence and/or history data			
Please describe:			☐

Provide details of data subjects - checking all that apply. Add any additional items in the 'other' option.			
Residents	☒	Customers/Clients/Citizens	☒
Children/young people	☐	Vulnerable people/groups	☒
Staff/employees/agency staff	☒	Volunteers	☒
Other: Please describe	☐		

Step 3a – Identifying risks & solutions

The following questions will highlight any risks associated with the principles of the UK General Data Protection Legislation (UK GDPR) and Data Protection Act 2018 (DPA) and other privacy legislation

Where a risk is identified, it should be carried forward to the table in Step 3b below, where mitigation and evaluation should be recorded. Suggestions/hints/tips are shown in italics		
Data protection/ privacy Issue	**Response**	**Risk (Yes/No)**
Who is the IAO and IAA?	Katie Peeke-Voute/Tania Weston, Nicola Grayson	N
How many individuals will be affected	The area is covered by two Lower Super Output Areas (LSOAs) that each consists of 1,600-3000 residents. Additionally, people pass along Walmgate into the city centre and along the City Walls and may wish to be kept informed. It is likely that the number of people wishing to be kept informed will be much lower than this.	Y
What is the nature of the relationship with the data subjects?	We will be conducting engagement with people to make sure improvement projects are supported locally. People who wish to be kept informed will need to provide contact details, email address by preference. In those cases where people do not have or want us to communicate with them by email we may collect phone numbers or postal addresses. We will only collect personal data if people have consented.	N
How will information be collected and/or what is the source of the information?	Email addresses	Y

	Where people do not/cannot provide an email address: name, phone number and/or postal address	
Who will have access to the information?	The CYC project team. Personal data will stored on the Regeneration Team channel. The document will be password protected.	N
Is any information shared within CYC?	Information will be shared between Regeneration and Communications /Communities.	Y?
Is any information shared externally with other organisations?	No	N
What is the lawful basis for processing personal data?	Article 6 ***(a) Consent:*** *the individual has given clear consent for you to process their personal data for a specific purpose.*	
What is the lawful basis for processing special categories of personal data	N/A	
What is the lawful basis for processing criminal conviction or offences including past criminal convictions or offences	N/A	
Will information be processed in a way that goes beyond an	No	N

individual's reasonable expectations?		
Do we have any previous experience of this type of processing?	Yes	Y
How will you tell the individuals about the use of their information?	The Regeneration Team privacy notice will be shared with participants before they sign up to our mailing list or provide any information.	N
Does the privacy notice cover the processing activities, or does it need amending?	Yes	N
If you are relying on consent to process personal information, how will this be collected and what will you do if it is not given or withdrawn?	Consent will be sought at the outset. If it is not given the information will not be collected, if it is withdrawn we will remove the data from our files and ensure that it is removed or destroyed in every location. The details will be removed from the spread sheet and a record of their removal will be made in the same sheet.	N
Purpose Limitation		
Have you identified all the purposes at Step 1 for which you will use information?	Yes	
Does the processing achieve your purpose(s)?	Yes	

Is there another way to achieve the same outcome?	We would continue to provide information via the CYC website, noticeboards and meetings, but we would not have a way to update the people who are interested in the project and want to be kept informed.	N
How will you ensure data minimisation i.e. only collecting/processing the minimum amount for the purpose(s)?	We will only take names/email addresses where necessary for gathering feedback/ opinions and advertising events.	Y
How will you ensure there is no “function” or processing creep?	We will only seek information which is necessary to our project and will not seek further information.	N
Can you ensure that the data collected is good enough for the intended purpose?	Yes, we will ask people to supply their data.	N
Is there any information that could be removed or anonymised without compromising the purpose(s) set out at Step 1?	We will only collect personal information in order to keep people updated. Any feedback gathered will be anonymised.	N
Accuracy		
Can the information be amended and/or deleted if required?	Yes	N
How will you ensure information used will be accurate and up to date?	It will be stored on OneDrive in a spreadsheet and will be kept up to date for the duration of the project. After that information will be deleted.	N

Have you established retention periods for the information?	*Intranet | Retention schedule (york.gov.uk)* The information will be retained for 2 years in line with council policy. In April 2028 we will review the contact details and if still required will contact the customers to ask if they would like to remain on the contact list or be removed. This will only be the case for individuals who have submitted their emails to be contacted for feedback/ to be kept up to date.	
Does the new processing/system allow you to delete information in line with the retention periods?	Yes.	
If there is a business need to retain information beyond the retention period, e.g. historical trend analysis, can the data be anonymised at this point?	N/A	
Have you checked if there is there a legal or other requirement to transfer the data at the end of the retention period for permanent preservation e.g. City or National Archives? If there is, how will this be done?	The data will not be transferred.	
How will it be destroyed/deleted or transferred?	It will be permanently deleted from Onedrive and all version history will be deleted.	

Security		
If required, has the information security technical checks/questions been completed and approved by ICT/ICT security? OR has it identified any risks?	N/A	
Where will the information be stored?	The Regeneration team's OneDrive folder, with managed access, which will be kept to the project team. The data sheet will be password protected.	
Does the new or current system/ procedure/processing provide adequate protection against security risks?	Yes	
What is the current state of technology in this area and/or are there any relevant advances in technology or security?	We will be using the council's Teams software	
What training and guidance is or will be given to staff?	Information Governance Training is mandatory for all staff on an annual basis.	
What data protection training has been undertaken by staff?	Information Governance Training is mandatory for all staff on an annual basis.	
If a third party is being used, what is the data protection relationship e.g. independent controllers, joint controllers,	N/A	

controller / processor, or processor/controller?		
If a third party is being used, is there a contract in place with the appropriate UK GDPR/DPA 2018 clauses and schedule if needed?	N/A	
If a third party is being used, how have you checked that their processes are UK GDPR/DPA 2018 compliant?	N/A	
Is the third party signed up to any approved code of conduct or certification scheme e.g.,	N/A	
International Transfers		
Will you transfer information outside of the EEA?	No	
If transferring data outside of the EEA, does the country/ organisation demonstrate an adequate level of data protection?	N/A	
If transferring information outside of the EEA, how will you ensure that the information is transferred securely?	N/A	
Will you be using 'Cloud Based' systems to store or transfer information? If so, where is the	Stored on the council's system.	

geographical location of the server and does the system demonstrate and adequate level of data protection?		
Rights of the Data Subject		
How will you manage rights of individuals requests e.g. Subject Access Requests (SARs), request to rectify data, request to be forgotten, objection to processing, restriction?	Requests will be logged and handled in line with council policies. Individuals will be informed of how they can request removal of personal data. Personal data will be removed from logs.	
Does the system involve automated decision making? If so, do you have a process in place to facilitate human intervention?	No	
Accountability		
As a result of this new or change to processing, do you need to update entries in the Information Asset Register (IAR)/ROPA etc?	No.	
As a result of this new or change to processing, do you need to update any Policies or Procedures?	No	
As a result of this new or change to processing, do you need to	No	

consider any Codes of Practice, regulatory guidance etc?		

Step 3b – Identifying risks & solutions

What are the risks and mitigations about data processing? Required information: privacy risks identified, mitigation/solution, evaluation (i.e. is the risk eliminated/reduced/accepted). Treat this in the same way as defining project risks but look at it from a customer and data point of view. It is good practice to include the risks identified here in the project or service area risk register so that they are monitored throughout the lifecycle of the project and/or service provision. Transfer any risks identified in Step 3a above into the below table, i.e. all those where Risk is Yes.		
Risk	**Mitigation / Solution(s)**	**Evaluation** *Is the risk eliminated, reduced, or accepted?*
It is possible that a large number of people wishing to be kept informed. There is a risk that this data could be accidentally revealed when sending out newsletters through not blind copying people.	Officers will be reminded of the need to only use 'blind copy' when sending out group emails.	Reduced
There is a risk that information collected could be accessed internally by officers not involved with the project	Personal information (e.g. email address lists) will be stored on a password-protected spreadsheet and only officers directly involved in the Regeneration, Communications and Communities teams will have access	Reduced

Personal/special categories data/criminal offence data transfer • More than is necessary • Not accurate / up to date • Not by secure methods	N/A	
Individuals/data subjects are not informed or can access their rights	Use of current privacy notice(s) and reviewed annually: information.governance@york.gov.uk Intranet | Data Protection, Privacy, and Information Governance (york.gov.uk) https://www.york.gov.uk/privacy/RegenerationTeam	Reduced
Data breaches: Personal information may be exposed, leading to identity theft or fraud, financial fraud, physical harm, or other forms of malicious use e.g.	Risk of data breach is medium: • All officers involved have completed staff training and will be reminded of the risk of accidentally not bcc'ing for mailing lists. • Data will be protected by use of passwords	Reduced
Breach notification obligations to ICO/NHS etc: If a data breach occurs due to insufficient security, the organisation may fail to meet its obligation to promptly notify affected individuals and relevant authorities.	• All officers involved have completed staff training	Reduced
Information could be accessed or shared without individuals' consent, violating their right to privacy.	• Data will be protected by use of passwords	Reduced

Non-compliance with data protection and privacy legislation/regulations resulting in regulator action/sanctions including potential fines and legal action.	• DPIA • DSA if needed • Privacy notices to be drafted/ reviewed • Compliance monitoring e.g. through internal audits etc	Eliminated
Improper system /records access	CYC organisational and technical measures such as • User designation and password approval, • user permissions limited based on access requirements for role	Reduced
Unlocked device with unauthorised access to system	CYC organisational and technical measures such as • Standard work policy to lock device when leaving desk. • Autolock • Rolling password changes	Reduced
Privacy notice does not reflect processing activity	Regeneration privacy notice recently reviewed and updated.	Eliminated
Retention periods are not adhered to	Annual review of retention periods and retention	Reduced
IAR/ROPA is not up to date	IAR/ROPA will be updated to include all new and updated assets and new processing activities	Reduced
Policies and procedures do not reflect new project/new or change to processing	• Annual review of policies/procedures • Changes flagged by relevant CYC team	Reduced
Regulatory investigations from concerns/complaints being raised to them and/or through their monitoring of all data controllers e.g. audit, inspect or investigate the council's DP/IG and ICT security practices, resulting in	• CYC ICT, information governance policies and procedures	Reduced

reputational damage and possible penalties for non-compliance.		
Financial loss from breaches and subsequent legal action and/or insurance claims from individuals could result in financial losses, including legal fees, fines, and compensation to affected individuals	• CYC ICT, information governance policies and procedures	Reduced
Inability to access services or opportunities	N/A	
Loss of control over the use of information;		
Discrimination	N/A	
Re-identification of pseudonymised data	N/A	
Loss of confidentiality	N/A	
Any other significant economic or social disadvantage	N/A	

Some other examples of actions that can reduce risks are

- taking additional technological security measures; or using a different technology; training staff to ensure risks are anticipated and managed.
- anonymising or pseudonymising data where possible.
- writing internal guidance or processes to avoid risks.
- putting clear data-sharing agreements into place with all partners.
- offering individuals the chance to opt out where appropriate; or
- implementing new systems to help individuals to exercise their rights

Step 5 – Record of outcomes and sign off

Please complete the sign off section below and email a copy of the full document to information.governance@york.gov.uk
Where it is identified that the processing is likely to result in a high risk to individuals, approval will need to be gained from the Senior Information Risk Owner and/or Chief Operating Officer and/or the Information Commissioner's Office. Please see Do we need to consult the ICO? | ICO

	Yes/No	Date	Name	Position
Confirm ongoing or outstanding actions will be integrated to the project or service plan with date and name and position of who responsible	Yes	05/06/26	Nicola Grayson	Regeneration Project Co-ordinator
Residual risks approved:	Yes	05/06/26	Tania Weston	Regeneration Programme Manager
DPO/Information Governance advice provided:				
Summary of DPO/ Information Governance advice:				
DPO/Information Governance advice accepted.				
If not accepted, please explain the reasons:				

Project/Process Sponsor

Name	Ben Murphy
Job Title	Head of City Development
Signature	
Date	

Information Asset Owner	
Name	Katie Peeke-Vout
Job Title	Head of Regeneration
Signature	
Date	

Data protection/information governance	
Name	
Job Title	
Signature	
Date	18/05/26