Data Privacy Impact Assessment

Overview
In carrying out a project that will use personally-identifiable information, whether collecting it or it is being given by a data provider, the research commissioner or data provider to may be asked or need complete a Data *Privacy Impact Assessment* (DPIA).

This document comprises two sections:

1. A set of screening questions, for people who are unsure whether or not they need to fill in a DPIA
2. A template form for a DPIA, based on guidance issued by the Information Commissioner's Office. This form guides you through many of the issues that need to be considered when conducting a DPIA

Section 1: Screening questions
The questions below are intended to help in deciding whether a DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise. Answers can be expanded as the project develops if needed.

NB – If you've been told by research data provider that you must fill in a DPIA, you can skip this section and go straight to the Data Privacy Impact Assessment form *on page 3.*

1. **Will the project involve the collection of new information about individuals?**
   Re-use of data collected for one purpose e.g. providing a service but now being used for research is covered by question 4.

2. **Will the project compel individuals to provide information about themselves?**
   This could occur if an organisation has commissioned a research project relating to staff.

3. **Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**
   This could also cover situations where an organisation is providing you with information for a research project that they haven't supplied to a third party before.

4. **Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**
   If you are re-using a research data set, then this question won't apply.

5. **Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.**
   This would cover things like fingerprint technologies.

6. **Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**
   If you are conducting research for an organisation that could affect their clients or staff, this may apply.

7. **Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.**
   Or any of the sensitive personal data, that is, ethnicity or racial origin, political beliefs, religious beliefs, trade union membership, sexual life.

8. **Will the project require you to contact individuals in ways that they may find intrusive?**
   This may vary from individual to individual e.g. some people are happy for their health records to be used for research, others only want them used for their health care.

9. **Has the research funder or data provider asked for the results of a Privacy Impact Assessment?**
   If you have not done a privacy impact assessment prior to this request, but are required to by a research funder or data provider, you will need to fill out this form.

Section 2: Data Privacy Impact Assessment Form

Step one: Identify the need for a DPIA

Swanley Town Council collects a variety of data from local residents, business, sponsors, service providers and other authorities. In some cases the information relates to information of a personal nature such as home address, telephone numbers, photographs and similar information. For this reason it has been identified that Swanley Town Council complete a Data Privacy Impact Assessment Form.

This will align new documents to existing policies and procedures used by the Town Council, including:

- Data Protection Policy
- Consent Form
- Privacy Statement (Staff)
- Privacy Statement (Public)
- Subject Access Request Form

As a small local authority Swanley Town Council has other legal obligations to provide services (such as allotments) which require the collection of personal data and while these services do not require the DPIA they still require an explanation of why, where and for how long data is being stored. As the tenants of these sites are constantly changing the council is collecting ‘new data’ which falls within the act.

Step two: Describe the information flows

Data collection come through 3 different sources and should always be accompanied by a consent form indicating what purpose the information is being provided for. There are currently no plans for the information gathered which relates to one project is then shared with another. i.e. those people purchasing tickets and services are NOT then contacted to take part in the Neighbourhood Plan.

Methods

1. Collected from Town Council employees directly (LINK, Venues)
2. Obtained via on line surveys created by Town Council employees
3. Obtained for other purposes by Consultants employed by STC

Data is only collected by consultants with the approval of the CEO and Civic Manager and supported by a letter indicating the purpose of the data capture and consent form

Consultation requirements

Swanley Tow Council will never pass on information to another organisation without the consent of an individual unless it has a legal obligation to do so i.e the information has been requested by an organisation legally enabled to do so, such as:

- HMRC
- Police
- Border Control
- SIA

We will regularly consult with staff and users to identify the needs of the organisation and to confirm compliance with the regulations in safe guarding the information held by STC, including:

- Payroll Provider
- I.T Provider
- CCTV Provider
- LINK providers
- Barclay Card
- STC Banking Provider

Step three: Identify the privacy and related risks

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

Annex 2 can be used to help you identify the GDPR related compliance risks.

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk		
Taking Photos of children	Loss of privacy and distress to individuals and parents if released	Can be requested under SAR loss of photography	Could prevent future capture of information for advertising purposes		
Taking photos of residents at events	Loss of privacy and distress if of a compromising nature	Can be requested under SAR loss of photography	Could prevent capture of promotional information		
Personal Information published on web site	Loss of privacy and distress and/or anti-social behaviour	Request to be 'Forgotten' could be lodged	Loss of personal detail which could affect income		
Release of personal statements made onto web site	Loss of privacy and potential for identifying political persuasion / ethnicity and similar	Request to be 'forgotten' work require substantial work from STC staff	Destroy trust in STC and negate future opportunities for working together		
Release of bank details and associated information on individuals	Loss of funds, release of personal income levels	Demand for compensation	Could have a serious detrimental effect of all services and staffing levels of STC		

Privacy issue	Risk to individuals	Compliance risk	Associated organisation / corporate risk	
Councillors compliancy	This is a legal compliance but could result in anti-social issues	Untested right to be forgotten both while in office and when term of office has finished	Could create a conflict with existing rules and regulations for councillors	
Staff information released such as salaries, address	Loss of privacy and compromised home life	Could lead to formal complaint and right to compensation	Has financial repercussions for STC	

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).

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?		
Taking Photos of children	Provide access to photos on site if requested and ensure consent forms are obtained	The photos would not be released outside the organisation without having obtained a consent form.	If not compliant there could be harm caused to children described as in care or at risk		
Taking photos of residents at events	Get consent forms first and provide signage at events that informs that photos are being take.	With consent forms the risk is eliminated. If general photos are provided then the risk is reduced	If not compliant then an individual may seek compensation under GDPR		
Personal Information published on web site	Consent forms available and this information is controlled by different staff. Collected and stored by a no internet access member of staff	Risk is minimalised through a no share policy between staff	Impact could release sensitive information which would leave the council open to claims for compensation under GDPR		

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).

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?			
Release of personal statements made onto web site	Consent forms available and this information is controlled by different staff. Collected and stored by a no internet access member of staff	Risk is minimalised through a no share policy between staff	This could leave the council open to claims for compensation under GDPR			
Release of bank details and associated information on individuals	Staff responsible for the web site and social media are different from those collecting personal data. There should never be an occasion when this information might be transferable	The risk is virtually eliminated as a result and staff training should ensure that this is 100% effective.	The impact on an individual could be significant in terms of financial loss and leave the council open to claims for compensation.			

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).

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?			
Councillors compliancy	This is currently a legal requirement for councillors elected into office where an individual has a sensitive job of function STC is able to provide the office as a contact source for control	The risk is that councillors may be targeted by individuals.	This is has been ever present and councillors are aware of the need to report instances. Associated issues will normally remain a police issue			
Staff information released such as salaries, address	Staff contact details are not published on web sites or social media. To provide some discretion only salary scales are indicated as required by LGA for those earning over £50,000	The risk to staff is greatly reduced but not eliminated from salary requirements to one or two individuals	This is proportionate to the need for LGA compliance and should not present a serious threat to any individual			

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
Taking Photos of children	Provide access to photos on site if requested and ensure consent forms are obtained	*Steve Nash*
Taking photos of residents at events	With consent forms the risk is eliminated. If general photos are provided then the risk is reduced	*Steve Nash*
Personal Information published on web site	Consent forms available and this information is controlled by different staff. Collected and stored by a no internet access member of staff	*Steve Nash*
Release of personal statements made onto web site	Consent forms available and this information is controlled by different staff. Collected and stored by a no internet access member of staff	*Steve Nash*
Release of bank details and associated information on individuals	Staff responsible for the web site and social media are different from those collecting personal data. There should never be an occasion when this information might be transferable	*Steve Nash*
Councillors compliancy	This is currently a legal requirement for councillors elected into office where an individual has a sensitive job of function STC is able to provide the office as a contact source for control	*Steve Nash*
Staff information released such as salaries, address	Staff contact details are not published on web sites or social media. To provide some discretion only salary scales are indicated as required by LGA for those earning over £50,000	*Steve Nash*

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

Who is responsible for integrating the DPIA 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	
Taking Photos of children	When requested: within 40 days of request being made	Local Manager i.e. Person organising activity	
Taking photos of residents at events	When requested: within 40 days of request being made	Local Manager i.e. Person organising activity	
Personal Information published on web site or social media	When requested: within 40 days of request being made	Civic Manager, Chloe King, Barbara Playfoot	
Release of personal statements made onto web site	When requested: within 40 days of request being made	Civic Manager, Chloe King, Barbara Playfoot	
Release of bank details and associated information on individuals	When requested: within 40 days of request being made	Steve Innes, Chloe King, Barbara Playfoot	
Councillors compliancy	When requested: within 40 days of request being made	CEO, Civic Manager Barbara Playfoot	
Staff information released such as salaries, address	When requested: within 40 days of request being made	Civic Manager, Barbara Playfoot	

Contact point for future privacy concerns
Primary Source of information Steve Nash acting as DPO

Annex 1

Primary contacts for advice and guidance

Steve Nash
CEO
GDPR Aware
snash@swanleytowncouncil.gov.uk

Toni Roast
HR Manager
GDPR Aware
troast@swanleytowncouncil.gov.uk

Steve Innes
RFO
GDPR Aware
sinnes@swanleytowncouncil.gov.uk

Claire Cormack
LINK Manager
GDPR Aware
ccormack@swanleytowncouncil.gov.uk

Question can also be asked via the .Gov web site GDPR Compliance

Annex 2

Linking the DPIA to the data protection principles

Answering these questions during the DPIA process will help identify where there is a risk that the project may fail to comply with the DPA or other relevant legislation, for example the Human Rights Act.

Principle 1

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:

a) at least one of the conditions in Schedule 2 is met, and

b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

Have you identified the purpose of the project?
Yes, this included in the information within this document and all annexes

How will you tell individuals about the use of their personal data?
This is published on our web site, social media and notice boards and when gathering data individuals will sign consent forms indicating how their data is to be used.

Do you need to amend your privacy notices?
This has been done with Privacy Notices for Staff and the Public

Have you established which conditions for processing apply?
Yes, as a local authority we gather information on related services which we are legally entitled to do. Staff are trained where appropriate in the gathering and disposal of data information.

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?
Data will be collected directly from town council employed staff. Where refusal of information is preferred then a service may be withheld if there is a legal need for us to hold such information. This will apply to tenancy agreements for allotments or accommodation and licenses or concessions.

If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?
We will remain mindful of Human Rights needs but are not legally obliged to comply.

Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data?
This is covered in the Privacy Statements and within the Consent for which is completed by every individual.

Have you identified potential new purposes as the scope of the project expands?
Where new services are brought on line and where additional types of information is sought for collection STC will make additional provision within our GDPR policy

Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?
STC collects data specific to its needs for processing payments, issues licenses, collecting fees and contacting interested parties. This information will be specifically provided by the individual concerned and will be accurately recorded from their input whether manually or electronically

Which personal data could you not use, without compromising the needs of the project?
There is no requirement for STC to obtain next of kin details relating to members of the Public but there is a need to hold this data for members of staff. This is collected by two separate departments and should not be released or compromise those involved in any way

Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?
STC holds a variety of software licenses that it regularly updates and employs and external consultant to install and amend.

How are you ensuring that personal data obtained from individuals or other organisations is accurate?
The information collected is provided directly to us by individuals and organisations. Contact details are checked within a matter of days where required and systems for payments automatically highlight discrepancies

Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.

What retention periods are suitable for the personal data you will be processing?
STC will destroy or remove data which is not required after a period. Those periods may be governed by other rules and regulations relating to the collection of information .i.e. Financial Records must be kept for a minimum period of 6 years. But personal information relating to tenancy is only kept where there is a financial link to records. Documents relating to Personal Injury Claims will be disposed of after a period of 3 years unless other correspondence relating to potential claims has been received.

Are you procuring software that will allow you to delete information in line with your retention periods?
Our software will allow us to time date information for deletion but some systems remain manual and will be reviewed annually upon renewal

Principle 6

Personal data shall be processed in accordance with the rights of data subjects under this Act.

Will the systems you are putting in place allow you to respond to subject access requests more easily?
Yes many of our systems will allow easier access to information but it is unlikely at this point in time that all manual systems will be transferred to digital. However, as technology moves forward and individuals prefer digital methods of providing information we will update our systems as finances allow.

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?
Individuals may opt out at any time after the advertising period has been completed in the first instance. Some of our advertising is annual and follows a generic pattern. A consent form will always be used when including an individual in an advertising campaign first but it would be cost prohibitive to exclude an individual during a campaign. It may be possible to anonymise an individual rather than remove them if there are concerns over safety.

Principle 7

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified?
STC have updated our I.T. systems and included bitlock software to provide password protected systems on each machine so that in the event a lap top or desktop are stolen all files remain protected. Sensitive information is also password protected by staff if it is listed as Confidential or above.

What training and instructions are necessary to ensure that staff know how to operate a new system securely?
Staff will have attended at least two training sessions in relation to GDPR. Training session one outlines the requirements of GDPR along with the rights of an individual and the rights of a member of staff. It outlines the councils obligations to members of the public and compliance details of the council. Training session two relates to the use of STC forms, the flow of data information and the responsibilities of Data Controllers and Data Processors.

Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Will the project require you to transfer data outside of the EEA?
Not at this time, however if any type of request is made we will ensure we follow procedures and confirm our obligations with the ICO at the time

If you will be making transfers, how will you ensure that the data is adequately protected?
All information we transfer between is bitlocker and password protected