Annex C - Data Protection Impact Assessment

Please send general queries about the DPIA process or form and / or return the form to DPO@bracknell-forest.gov.uk, copying in your IG Lead.

Title of DPIA	
	Procurement of a community hub operator for Buckler's Park
Brief summary of the project/ initiative	
	The department is seeking to agree the procurement process to appoint a suitable operator to manage the new Buckler's Park Community Hub, sports courts, changing rooms, car parking and associated landscaping.

Contact Details			
Author of this DPIA (Business owner) If the IG Lead is completing this document, the Business Owner should also be identified			
Name of Author	Ben Lawson		
Job Title	Community Hubs Project Manager		
Department/Team Name	Chief Executive's Office		
Email	ben.lawson@bracknellforest.gov.uk	Tel No.	07824618208
Business Owner (if different from Author)			
Project Sponsor/Director/Information Asset Owner			
Name	Abby Thomas		
Job Title	Assistant Director, Chief Executive's Office		
Date of submission	**17/03/2021**		

Purpose of a DPIA

The purpose of a DPIA is to assess the risks to people's personal data. By completing the steps in this DPIA, we identify, analyse and minimise the risk.

This DPIA is not a one-off exercise and recommendations should be added into project/ service plans. This DPIA should be reviewed per the DPIA Tracker (please contact your IG Lead or the DPO Mailbox if you are unsure).

When completing the DPIA think about the best interests of the data subject(s), security and protection measures you would want putting in place to address risk if it were your data!

Checklist - Initial Assessment

If you answer no to everything below you can stop here, it is unlikely that a full DPIA is needed. You must still send this form to the DPO Mailbox DPO@bracknell-forest.gov.uk **please copy in your IG Lead for awareness.**

If you answer yes to any of the following you must complete the remainder of this document. You must then send it to the DPO Mailbox DPO@bracknell-forest.gov.uk **please copy in your IG Lead for awareness:**

☐ use systematic and extensive profiling or automated decision-making to make significant decisions about people;
☐ process special-category data or criminal-offence data on a large scale;
☒ systematically monitor a publicly accessible place on a large scale;
☐ use innovative technology in combination with any of the criteria in the European guidelines;
☐ use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
☐ carry out profiling on a large scale;
☐ process biometric or genetic data in combination with any of the criteria in the European guidelines;
☐ combine, compare or match data from multiple sources;
☐ process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
☐ process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
☐ process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;
☐ process personal data that could result in a risk of physical harm in the event of a security breach;
☐ if there is a change to the nature, scope, context or purposes of our existing processing.

Procurement and Legal Advice

Procurement engagement, support and approval		
Is there a procurement aspect to your project/ initiative?	Yes ☒	No ☐
Has a member of BFC procurement been involved in developing this proposal?	Yes ☒	No ☐
If YES, name procurement professional: Keith Ashby		
If there is a procurement aspect, you must ensure Procurement have had input into this DPIA.		

ICT engagement, support and approval		
Is there an IT aspect to your project/ initiative?	Yes ☐	No ☒
Has an BFC ICT Business partner been involved in developing this proposal?	Yes ☐	No ☒
If YES, name the ICT Business Partner:		
If there is an ICT aspect, you must ensure ICT have had input into this DPIA.		

1. Project description

Provide a full description of the project, initiative or service

Please choose all of the below that apply to the project, initiative or service you are delivering

☒ The collection of new information about individuals

☒ Compelling individuals to provide information about themselves

☒ The disclosure of information about individuals to organisations or people who have not previously had routine access to the information

☐ The use of existing information about individuals for a purpose it is not currently used for, or in a way it is not currently used

☐ Contacting individuals in ways which they may find intrusive

☒ Making changes to the way personal information is obtained, recorded, transmitted, deleted, or held

☒ The use of profiling, automated decision-making, or special category data to make significant decisions about people (e.g. their access to a service, opportunity, or benefit)

☐ The processing of special category data or criminal offence data on a large scale

☒ Systematically monitoring a publicly accessible place on a large scale

☐ The use of new technologies

☐ Carrying out profiling on a large scale

☐ Processing biometric or genetic data

☐ Combining, comparing, or matching data from multiple sources

☐ Processing personal data without providing a privacy notice directly to the individual

☐ Processing personal data in a way which involves tracking individuals' online or offline location or behaviour

☒ Processing children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them

☐ Processing personal data which could result in a risk of physical harm in the event of a security breach

What are the project's objectives/ scope/ benefits?

The council has been working with Crowthorne Parish Council to develop a community hub at the former Transport Research Laboratory site in line with the Executive's

decision in September 2014 that the Council's preferred policy for the development of the new community hubs is to transfer these into the ownership and management of the Parish and Town Councils or other third party.

Nature of personal information							
Forename	☒	Surname	☒	Postal address	☒	Post code	☒
Email address	☒	Age	☒	Date of Birth	☒	Gender	☒
Mobile Number	☒	Telephone Number	☒	NI Number	☐	NHS number	☐
Unique ID number (e.g. Mosaic ID)	☐	Online identifier (IP address etc.)	☐	Voice recording	☐	Image (photo or video of person)	☒
Personal financial details	☐	No personal data held	☐				
Other:							

Which of the following special category data will be used							
Criminal allegations convictions or offences	☐	Data concerning health information	☐	Data concerning sex life or orientation	☐	Religious or philosophical beliefs	☒
Political opinions	☐	Racial or ethnic origin	☐	Biometric data	☐	Genetic data	☐
Trade Union membership	☐	No special category data	☐				

Number of individuals with which personal data will be processed

0 - 100	☐
100 - 1000	☐
1000 – 5000	☒
5000 +	☐

What geographical area does it cover?

UK	☒
EU	☐
International	☐

2. Describe the processing

Describe the nature of the processing
How will you collect, use, store and delete the data?

Collect;
Data will be collected by the proposed operator, managing access and membership to the community hub.

Use;
The data will be used for confirmation of centre user's identification within the same context as using the facilities at a leisure centre or library.

Store;
The data will be stored on the operator's database.

Delete;
In accordance with BFC retention schedule, assessment data will be held for 6 years after the date that the case is closed. See https://www.bracknell-forest.gov.uk/sites/default/files/documents/retention-schedule.pdf

What is the source of the data?
The applicant / member of the community hub and/or their parent's, guardians, teachers carers and anyone else who would provide a supporting role to the facilities user.

Will you be sharing data with anyone?

Yes	☒
No	☐

If yes, please list who you will be sharing the data with

The hub's operator and potentially secondary operators

Describe the scope of the processing

How often will you be collecting personal data?

Daily	☒
Weekly	☐
Monthly	☐
Annually	☐
Other	

How long will you keep it?
If this is different for different types of data, you can choose more than one and describe each in the text box below

0 – 1 year	☒

1 – 5 years	☒
5 – 10 years	☐
10 – 20 years	☐
Indefinitely	☐
Other	☐

0-1 year for one-off visits, 1-5 years for membership for the use of the hub's facilities

Describe the context of the processing

What is the nature of your relationship with the individuals?

The individuals will be residents or users of BFC / Crowthorne Parish Council facilities or amenities who will need to log their personal details at the hub for fire safety, membership and security purposes.

Is there another way to achieve the same outcome you are trying to reach?

No

How much control will individuals have?

This would have to be assessed on an individual basis due to the expected diverse range of individuals using the facilities.

Do the individuals include children or other vulnerable groups?

Yes, children and vulnerable adults

Are there prior concerns or security flaws around this type of processing?

Yes, the possibility of a 'lack of vigilance' from the hub operator regarding the use of personal information.

Is the processing novel in any way?

No

What is the current state of technology in this area?

Details will be stored primarily on a database ran by the operator, adhering to BFC's GDPR requirements and protocols

Are there any current issues of public concern that you should factor in?

No, providing information management follows BFC's GDPR protocols

Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Not yet

What is the retention period for this information?

In accordance with BFC retention schedule, assessment data will be held for 6 years after the date that the case is closed. See https://www.bracknell-forest.gov.uk/sites/default/files/documents/retention-schedule.pdf

How will this information be deleted/ destroyed?
Secure disposal

3. Consultation process

Consider how to consult with relevant stakeholders

Describe when and how you will seek individuals' views, or justify if it is not appropriate to do so.
The DPIA covers a plan to collect the personal data of individuals not yet identified.

Describe when and how you have consulted partner organisations, or explain why it is not appropriate to do so.
Partner organisations have not been contacted yet due to the sensitivities relating to the procurement structure of the potential tender process.

Who else have you involved within the Council?
No department yet but the operator will adhere to BFC's GDPR protocols which will be included within the tender document and contractually binding.

Do you have a processor? Do you need to ask your processors to assist?
No

Do you plan to consult information security experts, or any other experts?
No

Do you have a relevant privacy notice that includes this processing? How will you actively provide this privacy information to individuals?
The Council's privacy notices are available to view on the Council external website

4. Compliance and Proportionality

To be completed with guidance from Legal Services if necessary

What is your lawful basis for processing?
☐ Public task: we need to process the data to perform a specific, necessary task that is in the public interest and is set out in law ☐ Consent: the data subject consents to the processing of their personal data ☐ Contract: we need to process the data to fulfil our contractual obligation with the individual ☐ Legal obligation: we need to process the data to comply with the law ☐ Vital interest of the data subject: we need to process the data to protect the individuals' life ☐ Legitimate interest (as a public body, this basis is very unlikely to apply and you must complete the Legitimate Interest Assessment before choosing this)
If you have chosen legal obligation or public task, identify the legislation / authority (e.g. Children Act (2004), Health and Social Care Act (2012) Crime and Disorder Act (1998))
N/A

Does the processing actually achieve your purpose?
Yes

How will you prevent function creep?
All Bracknell Forest staff are required to complete mandatory data security training as part of their induction as well as ongoing refresher courses. Data protection issues will be discussed in contract monitoring with the hub operator.

How will you ensure data quality and data minimisation?
Details of members and visitors will be subject to the same processes that similar facilities use within the constraints of BRC's GDPR procedures.

What information will you give individuals (e.g. a relevant Privacy Notice)?
The operator must demonstrate to the individuals their commitment to GDPR as an assurance of the operator's competence.

How will you help to support individuals' rights (e.g. inform them of their data rights)?
People will be advised of the privacy policy and about how their personal data will be used. Requests to access data can be made in line with the providers and BFC's privacy policy.

What measures are in place to ensure processors comply with relevant data protection requirements?
Contract monitoring and training if required

Do you make any international transfers? If, so what safeguards are in place?
N/A

5. Risk Review – Identify measures to reduce risk (to be completed by business owner with support from Audit and Risk Management if needed)

The following is the Council's risk assessment matrix. It combines a risk rating from low to very high, derived from a combination of the likelihood of a risk occurring, coupled with the impact if it does. It, and the Likelihood and Impact scoring guides below should be used to assign pre and post mitigation risk scores in the risk log in the following section.

RISK MATRIX

LIKELIHOOD						
	5	Medium	High	High	High	High
	4	Medium	Medium	High	High	High
	3	Low	Medium	Medium	Medium	High
	2	Low	Low	Low	Medium	Medium
	1	Low	Low	Low	Low	Medium
		1	**2**	**3**	**4**	**5**

IMPACT

Likelihood:
5 Very High
4 High
3 Significant
2 Low
1 Almost Impossible

Impact:
5 Catastrophic 80%+
4 Critical 51% – 80%
3 Major 21% – 50%
2 Marginal 6% – 20%
1 Negligible 0% – 5%

	The risk log below should detail privacy risks that the project/initiative may give rise to; mitigations with completion dates; pre and post-mitigation risk ratings and mitigation action owners (i.e. the name of the person who is responsible for carrying out the actions required to mitigate the risk(s). The Information Asset Owner / Project Sponsor etc. will be accountable for ensuring the mitigations are completed. Mitigating actions should be incorporated in project plans. **This information should be incorporated into the project plan/ proposal documentation** **KEY: L** = Likelihood of the risk occurring **I** = Impact of the risk occurring [see BFC risk matrix to apply scoring 1 to 5 in each case to drive a score]										
#	**Risk Description** **There is a risk that …. Giving rise to ….**	**Pre-Mitigation**			**Mitigating Action(s) and**	**Action Owner (i.e. who is responsible for the action)**	**Due Date**	**Status**	**Post-Mitigation**		
		L	**I**	**Risk**					**L**	**I**	**Risk**
e.g. only	Mobile equipment (laptops) will be lost resulting in loss of / unauthorised access to personal data	4	5	H	Laptops to be encrypted by ICT prior to roll-out. Reporting system for lost equipment in place	Claire Smith	30/9/18	Live	2	4	M
e.g. only	Data will be accessed by people who are not authorised to view it resulting in increased privacy risks	5	3	H	Access controls to be set within CareCounts system and administered by X. Reports will be generated every X months and access will be checked by Y with action taken accordingly.	Robert Patel	31/12/18	Live	2	3	L
1	Mobile equipment may be lost or stolen, resulting in loss of / unauthorised access to data	4	5	H	All BFC mobile devices (laptops, tablets, phones) should be encrypted and password protected to prevent unauthorised use. Personal data should not be stored on the hard drive itself but directly entered to the record system (i.e. LAS). All staff at BFC are trained re: data protection measures as part of induction and regular refresher courses; instructed not to leave items on display in cars etc. where they may be at risk of theft.	Ben Lawson					

2	Personal data around a care home placement is emailed to the incorrect recipient, or via an unsecured channel	4	3	H	All BFC staff undergo mandatory information security training to limit the possibility of such incidents and are also trained in how to deal with the situation should an incident occur. The operator will be contractually obliged to follow suit or provide a suitable training mechanism to reflect the GDPR processes.	Ben Lawson					
3	Hub operator's system compromised by ransomware or other cyber attack	3	5	M	Operator should demonstrate that a spam filter is in operation to prevent suspicious emails. Any email from an external source should be flagged with a caution to be wary of malicious links/attachments. Staff will also be trained regarding suspicious links in emails as part of induction and receive reminders from ICT to be mindful of attacks. Provider's data security procedures to be confirmed during contract process.	Ben Lawson					
4	The operator fails to exercise good data protection practices, putting personal data at risk	3	4	H	The council to seek confirmation that the supplier does exercise good data protection practices.	Ben Lawson					
5	The provider has ICO enforcement notices or decision notices issued against them	2	4	M	To be identified through contract monitoring and management	Ben Lawson					

8. Sign-Off, Advice and Approvals

Business Owner Sign-off This DPIA is an accurate account of the project / initiative and Data Protection and Security measures that will be applied. Outstanding risk mitigations will be incorporated into project plan or service delivery.			
Comments: Click or tap here to enter text.			
Name		**Date**	Click here to enter a date.
Signature			

DPO Sign-off The DPO's advice is based on an assessment of the DPIA and whether proportionate and appropriate technical and organisational measures have been put in place to uphold an individuals' right to privacy.
Recommendation, comments and sign-off
Accept that no full DPIA is required ☐ DPO comments/rationale as to why no full DPIA required: Click or tap here to enter text. Date of sign off:
Approve full DPIA as drafted ☐ DPO comments/advice: Click or tap here to enter text. Date for review: Date of sign off:
Approve full DPIA subject to conditions ☐ Conditions and rationale: Click or tap here to enter text. Date for review: Date of sign off:
Reject full DPIA as drafted ☐ DPO comments/advice: Click or tap here to enter text. Date of next DPO review:

Refer full DPIA to ICO ☐

Reason for referral to ICO:

Click or tap here to enter text.

Date of referral:

ICO response:
Click or tap here to enter text.

Actions taken and next steps:
Click or tap here to enter text.

DPO request for assurance from Legal Services		
Legal advice sought?	Yes ☐	No ☐

Legal advice/ recommendations

Click or tap here to enter text.

Advised by	
Date advice received	

SIRO/Caldicott Guardian decision

Before signing the DPIA, the SIRO/Caldicott Guardian must ensure that they have considered advice of the DPO and are satisfied that the impact assessment is robust, has addressed all the relevant issues and that appropriate actions have been taken. Where the advice of the DPO has not been accepted, the rationale should be set out below.

Caldicott Guardian Decision, comments and sign-off

Have you considered and accepted the DPO's recommendation?

Yes ☐

No ☐

If no, please record rationale:
Click or tap here to enter text.

Approve DPIA as drafted ☐

Caldicott Guardian comments/advice:
Click or tap here to enter text.

Approve DPIA subject to conditions ☐

Conditions and rationale:
Click or tap here to enter text.

Date for review:
Date of sign off:

Reject DPIA as drafted ☐ Caldicott Guardian comments/advice: Click or tap here to enter text.
Refer to ICO ☐ Reason for referral to ICO: Click or tap here to enter text. Date of referral: ICO response: Click or tap here to enter text. Actions taken and next steps: Click or tap here to enter text.

SIRO Decision, comments and sign-off
Have you considered and accepted the DPO's recommendation? **Yes** ☐ **No** ☐ If no, please record rationale: Click or tap here to enter text.
Approve DPIA as drafted ☐ SIRO comments/advice: Click or tap here to enter text.
Reject DPIA as drafted ☐ SIRO comments/advice: Click or tap here to enter text.
Approve DPIA subject to conditions ☐ Conditions and rationale: Click or tap here to enter text. Date for review: Date of sign off:
Refer to ICO ☐ Reason for referral to ICO:

Click or tap here to enter text.

Date of referral:

ICO response:
Click or tap here to enter text.

Actions taken and next steps:
Click or tap here to enter text.

DPIA approval details logged on the DPIA tracker	Click here to enter a date.

Document	**Title/Summary**
Legal Including: Information Security Questionnaires; Privacy Notices, Consent Forms, Information Sharing Agreements, Data Processing Agreements, documentation of suitable safeguards for transfers of personal data to a third country or an international organisation	
	[Embed Doc]
	[Embed Doc]
Project Including: Business cases, PIDs, training documents, procedures	
Design & ICT Security Including: Spec, Security Assessments, Network Diagrams etc.	
	[Embed Doc]
	[Embed Doc]
Procurement Including: IG evaluation(s), Contract/Agreement	
	[Embed Doc]
	[Embed Doc]