Data Protection Impact Assessment (DPIA) Template

A DPIA is designed to describe your processing and to help manage any potential harm to individuals in the use of their information. DPIAs are also important tools for demonstrating accountability, as they help you as a Controller to comply with the requirements of the Data Protection Legislation. Non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA at all, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

DPIA's are not new; the use of Privacy Impact Assessments has become common practice in the NHS and can provide evidence of compliance within the Data Security and Protection toolkit (DSPT); DPIAs build on that practice.

It is not always clear whether you should do a DPIA or not but there are a number of situations where a DPIA **should** be considered or where a DPIA is a **legal requirement**. If you can tick against the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, ensure that you document the reasons for your decision.

You as Controller **MUST** carry out a DPIA where you plan to:	Tick or leave blank
Use **profiling or automated decision-making** to make significant decisions about people or their access to a service, opportunity or benefit;	☐
Process **special-category data or criminal-offence data on a large scale**;	☐
Monitor a publicly accessible place on a large scale;	☐
Use **innovative technology** in combination with any of the criteria in the European guidelines;	☐
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.	✓

You as Controller should **consider** carrying out a DPIA where you	Tick or leave blank
Plan any major project involving the use of personal data;	✓
Plan to do evaluation or scoring;	☐
Want to use systematic monitoring;	☐
Process sensitive data or data of a highly personal nature;	☐
Processing data on a large scale;	☐
Include data concerning vulnerable data subjects;	☐
Plan to use innovative technological or organisational solutions;	☐

A new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

There is guidance to help you. Your Data Protection Officer (DPO) can be consulted before completing a DPIA in order to provide specialist advice and guidance or simply to talk things through with you.

Background Information	
Date of your DPIA :	12/07/2023
Title of the activity/processing:	BOB ICB New ID Badges
Who is the person leading this work?	[redacted]
Who is the Lead Organisation?	BOB ICB
Who has prepared this DPIA?	[redacted]
Who is your Data Protection Officer (DPO)?	[redacted]
Describe what you are proposing to do: (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	Following the creation of the new organisation the Digital Team has been tasked with obtaining new BOB ICB ID badges for all staff & contractors. BOB ICB badges will be used as the primary identification for BOB ICB employees. Passes will be generated and distributed following completion of the organisational change consultation. The new badges will be ordered from a chosen supplier outside of the NHS chain. This supplier will be provided with employee data Name, Surname, Job Title, and Photo. The below process has been agreed with HR by the Digital Team. **Collection of data for badges (will begin once HR confirms the job titles and organisational roles within BOB)** 1. It has been agreed that once the consultation process is complete and the BOB ICB directorates are formed, the BOB ICB HR team will provide the Digital Team with a report from the ESR system. The report will include a list of all BOB ICB employees stating their unique assignment number, name, job title, and base location, plus any other information required if previously agreed. The report would be prepared in excel. **Phase 1 – Bulk order** 1) HR to set up a secure location (Sharepoint) to store staff data collected for the ID Badge project. 2) HR to send a request to Directors for the name of a designated admin person who will be responsible for the administration of the ID Badge process within their directorate. 3) HR to produce list of staff details broken down by directorate. 4) HR to set up secure separate locations (Sharepoint) for each directorate which will be used to store the staff data. 5) Access to the secure location (Sharepoint) will be allocated by HR. Each designated admin person will only

	have access to their directorates secure location (Sharepoint). HR and the Digital Team will have access to all secure locations. 6) The designated admin person from each directorate will be required to save the staff data collected to the secure location (Sharepoint), to be used in the creation of ID Badges. 7) Once HR receives details of all designated admin persons from the Directors, this will be forwarded to the Digital Team, after which: a) a meeting will be set up to provide them with details of the ID Badge process and what they need to do to keep data secure. b) they will provide with the drafted staff communication to be sent to all staff via NHS email. 8) Comms to designated admin person to include: a) the named secure location (Sharepoint) the designated admin person will have access to and the link to access it. b) access to the staff data spreadsheet, how confirm staff details and instructions on how to upload photos. c) instructions on how the data requested from staff is to be returned to the designated admin person via NHS mail with data included in the attachment. d) instruction for the admin person to delete received data from their email inbox once received and saved in the secure location. e) draft communication to each employee specifying the request to collect confirmation of title, current job title and photograph (specification will be provided on what type of photo is required) of the employees in their directorate. This communication will also include: • link to Staff Privacy Notice, BOB ICB for full explanation of compliance. • specific advice to return data safely via NHS Email with the required data provided in the attachment of the email. • instruction to remove the data from their email after sending. f) The designated admin person will be instructed to remove the data once it is stored in the secure location (Sharepoint). 9) Once all data has been collected on the secure location (Sharepoint) it will be sent via secure NHSmail Egress to the ID Badge supplier ID Card Centre.

	10) On receipt of the staff data the ID Card Centre, they will proceed with data processing as per below: a) data will be saved to their Server based at HQ from where it will only be accessible by specific/designated members of the Team who have received full GDPR and information security training. b) data will be only used for the purpose of processing the pictures (adjusting the size if required) and printing the ID Badges. c) once data has been printed and the cards shipped out, the data will be kept on their server for 30 days to ensure that if there are any further adjustments/changes/ corrections required there is access to the data by ID Card Centre. d) after the 30 days the data is purged and permanently deleted. e) ID Badges will be shipped via insured package using UPS Courier to designated secure office location (NHS Berkshire West CCG Offices, 59 Bath Rd, Reading RG30 2BJ) where package will be signed for at the Reception Desk. 11) Once the ID Badges are delivered to the office the Reading, the Receptionist will place them in a secure location for the Digital Team/Admin person to collect. 12) Reading Receptionist to contact Digital Team via email to let them know a package is waiting for collection. 13) Initial batch of ID Badges received in Reading will be collected by Digital Team and sorted into Directorate/Dept batches. Digital Team will contact designated admin persons via email to inform them about badges awaiting collection. 14) Once the Digital Team have notified the designated admin person, it is their responsibility to collect and distribute ID Badges to the employees in their Directorate/Dept. 15) Once the ID Badges are received in the Reading office or by the Manager the data held will only be kept in the HR secure location (Sharepoint) for further orders. **Phase 2 – Process for BOB ICB ID Badges - New Staff Request/Replacements and Returns** 16) For any further ID Badges requests e.g. for new employees or replacements badges for existing employees the ID Badge form will need to be completed. For new employees the form will be provided as part of onboarding process. 17) The manager to ensure that the employee will be provided with the ID Badge form to complete. Once the

	form is completed, Manager to ensure that the form is sent to HR for filing and that the new badge is requested using the submitted form. 18) HR will update the ESR spreadsheet with the new details/new employee details. 19) To order a new badge/replacement badge the Manager will send the form to the ID Centre via secure NHSmail Egress to the provided by ID Card Centre email. 20) The Manager will include details of the secure location where the ID Badge is to be delivered. 21) The ID Card Centre to let the Manager know by e-mail when the ID Badge has been despatched. 22) The Manager will be responsible for receiving/collecting and distributing the Id Card Badges. **Reporting the lost badge** Employee will be obligated to notify the Manager about loss of the badge, who in turn notifies HR and Counter Fraud.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is)**.**	No
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	No
Detail anything similar that has been undertaken before?	Not aware of anything.

1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use

1.1.

What data/information will be used? Tick all that apply.	Tick or leave blank	**Complete**
Personal Data	✓	1.2
Special Categories of Personal Data	☐	1.2 AND 1.3
Personal Confidential Data	☐	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data)	☐	1.2 but speak to your IG advisor first
Pseudonymised Data	☐	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	☐	Consider at what point the data is to be anonymised
Commercially Confidential Information	☐	Consider if a DPIA is appropriate
Other	☐	Consider if a DPIA is appropriate

1.2.

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:

a) THE DATA SUBJECT HAS GIVEN CONSENT	**Tick or leave blank**
	☐

Why are you relying on consent from the data subject?
Because the personal data includes picture and full name details of the employee.

What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom).

Describe how your consent form is compliant with the Data Protection requirements? (There is a checklist that can be used to assess this).
It will include reference to the Privacy Notice.

b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY (The contract needs to be between the Controller and the individual and not concern data being processed due to someone else having a contract with the Controller. Processing can happen before the contract is entered into e.g. processing a pre-health assessment for a private or cosmetic procedure that is a paid for service with the delivery of that care done under contract between the Patient and the Practitioner).	**Tick or leave blank** ✓

What contract is being referred to?
within the Terms and Conditions of Employment. Signed on commencement of employment by the employee and signposted in Staff Zone - **Staff Privacy Notice, BOB ICB**

c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT (A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).	**Tick or leave blank** ☐

Identify the legislation or legal obligation you believe requires you to undertake this processing.
Click here to enter text.

d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON (This will apply only when you need to process data to protect someone's life. It must be necessary and does not only relate to the individual whose data is being processed. It can also apply to protect another person's life. Emergency Care is likely to fall into this category but planned care would not. You may need to process a Parent's data to protect the life of a child. The individual concerned is unlikely to be able to provide consent physically or legally; if you are able to gain consent then this legal basis will not apply).	**Tick or leave blank** ☐

How will you protect the vital interests of the data subject or another natural person by undertaking this activity?
Click here to enter text.

e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER (This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply).	**Tick or leave blank** ☐

What statutory power or duty does the Controller derive their official authority from?
Click here to enter text.

f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY (Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. See the guidance for more information about the legitimate interest test).	**Tick or leave blank** ☐

What are the legitimate interests you have?
Click here to enter text.

Article 9 (2) conditions are as follows:

a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	**Tick or leave blank** ☐
b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT (Requirements for this are the same as those detailed above in section 1.2, d))	**Tick or leave blank** ☐
d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members	*NA*
e) The data has been made public by the data subject	*NA*
f) For legal claims or courts operating in their judicial category	*NA*
g) SUBSTANTIAL PUBLIC INTEREST (Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
h) PROCESSING IS NECESSARY FOR THE PURPOSES OF PREVENTIVE OR OCCUPATIONAL MEDICINE, FOR THE ASSESSMENT OF THE WORKING CAPACITY OF THE EMPLOYEE, MEDICAL DIAGNOSIS, THE PROVISION OF HEALTH OR SOCIAL CARE OR TREATMENT OR THE MANAGEMENT OF HEALTH OR SOCIAL CARE SYSTEMS AND SERVICES ON THE BASIS OF UNION OR MEMBER STATE LAW OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐
j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT. (Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	**Tick or leave blank** ☐

1.3.

If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6. You must select at least 1 from a) to c) or g) to i). NOTE: d), e) and f) are not applicable

1.4.

Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role

BOB ICB	Sole Controller
ID Card Centre	Processor
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.

1.5.

Describe exactly what is being processed, why you want to process it and who will do any of the processing?

Personal data of Employee name including surname, job title and photo to be processed by ICB Digital Team, HR (collection and storage of data) and the ID Card Centre to process the data (produce the badges). The data will be delivered to the ID Card Centre via **NHSmail Egress** (cloud storage service as described above).

1.6.

Tick here if you owe a duty of confidentiality to any information. ✓

If so, specify what types of information. (e.g. clinical records, occupational health details, payroll information)

Employee name, surname, job title and photo.

1.7.

How are you satisfying the common law duty of confidentiality?

Consent – Implied

ID badges are for the identity of the employee while performing their duties including access to the building.

If you have selected an option which asks for further information, please enter it here.

1.8.

Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?

No

If you are then describe what you are doing.

If you don't know then please find this information out as there are potential privacy implications with the processing.

1.9.

Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care. ✓

If so describe that purpose.

For the purpose of creating ID Badges for BOB ICB staff members.

1.10.

Approximately how many people will be the subject of the processing?

100 plus

1.11.

How are you collecting the data? (e.g. verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)

By e-mail
Electronic form
Choose an item.
Choose an item.
Choose an item.

If you have selected 'other method not listed' describe what that method is.

Click here to enter text.

1.12.

How will you edit the data?

Data collected will be edited as follows:
-If the employee requested or agreed, the team will change first names to "known as" or shortened form of the name.
-Role titles maybe abbreviated, if needed.
-Resizing of pictures to fit badges, if needed.
All of the above will be agreed with employees during the data collection process.
Editing will be carried out by the Administrator of each Directorate, Digital Team/HR and the supplier, ID Card Centre.

1.13.

How will you quality check the data?

By requesting confirmation of data from individual employees. By having two check points Administrators of each Directorate and Digital Team/HR

1.14.

Review your business continuity or contingency plans to include this activity. Have you identified any risks?

Yes

If yes include in the risk section of this template. Risks added to 5.1 below.

1.15.

What training is planned to support this activity?

None, not necessary.

2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital

2.1.

Are you proposing to combine any data sets?

Yes

If yes then provide the details here.

Data provided by HR to be combined with the photos submitted from the Administrator of each Directorate.

2.2.

What are the Data Flows? (Detail and/or attach a diagram if you have one).

Phase 1 – Bulk order

23) HR to set up a secure location (Sharepoint) to store staff data collected for the ID Badge project.

24) HR to send a request to Directors for the name of a designated admin person who will be responsible for the administration of the ID Badge process within their directorate.
25) HR to produce list of staff details broken down by directorate.
26) HR to set up secure separate locations (Sharepoint) for each directorate which will be used to store the staff data.
27) Access to the secure location (Sharepoint) will be allocated by HR. Each designated admin person will only have access to their directorates secure location (Sharepoint). HR and the Digital Team will have access to all secure locations.
28) The designated admin person from each directorate will be required to save the staff data collected to the secure location (Sharepoint), to be used in the creation of ID Badges.
29) Once HR receives details of all designated admin persons from the Directors, this will be forwarded to the Digital Team, after which:
    a) a meeting will be set up to provide them with details of the ID Badge process and what they need to do to keep data secure.
    b) they will provide with the drafted staff communication to be sent to all staff via NHS email.
30) Comms to designated admin person to include:
    a) the named secure location (Sharepoint) the designated admin person will have access to and the link to access it.
    b) access to the staff data spreadsheet, how confirm staff details and instructions on how to upload photos.
    c) instructions on how the data requested from staff is to be returned to the designated admin person via NHS mail with data included in the attachment.
    d) instruction for the admin person to delete received data from their email inbox once received and saved in the secure location.
    e) draft communication to each employee specifying the request to collect confirmation of title, current job title and photograph (specification will be provided on what type of photo is required) of the employees in their directorate. This communication will also include:
        - link to Staff Privacy Notice, BOB ICB for full explanation of compliance.
        - specific advice to return data safely via NHS Email with the required data provided in the attachment of the email.
        - instruction to remove the data from their email after sending.
    f) The designated admin person will be instructed to remove the data once it is stored in the secure location (Sharepoint).
31) Once all data has been collected on the secure location (Sharepoint) it will be sent via secure NHSmail Egress to the ID Badge supplier ID Card Centre.
32) On receipt of the staff data the ID Card Centre, they will proceed with data processing as per below:
    a) data will be saved to their Server based at HQ from where it will only be accessible by specific/designated members of the Team who have received full GDPR and information security training.
    b) data will be only used for the purpose of processing the pictures (adjusting the size if required) and printing the ID Badges.
    c) once data has been printed and the cards shipped out, the data will be kept on their server for 30 days to ensure that if there are any further adjustments/changes/ corrections required there is access to the data by ID Card Centre.
    d) after the 30 days the data is purged and permanently deleted.

e) ID Badges will be shipped via insured package using UPS Courier to designated secure office location (NHS Berkshire West CCG Offices, 59 Bath Rd, Reading RG30 2BJ) where package will be signed for at the Reception Desk.

33) Once the ID Badges are delivered to the office the Reading, the Receptionist will place them in a secure location for the Digital Team/Admin person to collect.
34) Reading Receptionist to contact Digital Team via email to let them know a package is waiting for collection.
35) Initial batch of ID Badges received in Reading will be collected by Digital Team and sorted into Directorate/Dept batches. Digital Team will contact designated admin persons via email to inform them about badges awaiting collection.
36) Once the Digital Team have notified the designated admin person, it is their responsibility to collect and distribute ID Badges to the employees in their Directorate/Dept.
37) Once the ID Badges are received in the Reading office or by the Manager the data held will only be kept in the HR secure location (Sharepoint) for further orders.

Phase 2 – Process for BOB ICB ID Badges - New Staff Request/Replacements and Returns

38) For any further ID Badges requests e.g. for new employees or replacements badges for existing employees the ID Badge form will need to be completed. For new employees the form will be provided as part of onboarding process.
39) The manager to ensure that the employee will be provided with the ID Badge form to complete. Once the form is completed, Manager to ensure that the form is sent to HR for filing and that the new badge is requested using the submitted form.
40) HR will update the ESR spreadsheet with the new details/new employee details.
41) To order a new badge/replacement badge the Manager will send the form to the ID Centre via secure NHSmail Egress to the provided by ID Card Centre email.
42) The Manager will include details of the secure location where the ID Badge is to be delivered.
43) The ID Card Centre to let the Manager know by e-mail when the ID Badge has been despatched.
44) The Manager will be responsible for receiving/collecting and distributing the Id Card Badges.

Reporting the lost badge

Employee will be obligated to notify the Manager about loss of the badge, who in turn notifies HR and Counter Fraud.

2.3.
What data/information are you planning to share?
Name, surname, job title and photo with the supplier.

2.4.
Is any of the data subject to the National Data Opt Out?
No - it is not subject to the national data opt out

If your organisation has to apply it describe the agreed approach to this
Click here to enter text.

If another organisation has applied, it add their details and identify what data it has been applied to
Click here to enter text.

If you do not know if it applies to any of the data involved, then you need to speak to your Data Protection Officer to ensure this is assessed.

2.5.
Who are you planning to share the data/information with?

1. Digital Team to send ESR spreadsheet and pictures to ID Card Centre via secure NHSmail Egress.
2. ID Card Centre data process steps:
    - Data is downloaded and saved to the ID Card Centre Server based at HQ
    - Once on the server, the data is only accessible by specific members of the Team who have received full GDPR and information security training.
    - Once data has been printed and the cards shipped out, the data is kept on the ID Card Centre server for 30 days.
    - After the 30 days the data is purged and permanently deleted.
    - With regards to shipping the ID cards. All orders will be shipped by UPS insured service courier.
3. ID Card Centre if required, will edit pictures before producing the ID Badges for BOB ICB employees.
4. ID Card Centre to ship the orders to designated secure office location (NHS Berkshire West CCG Offices, 59 Bath Rd, Reading RG30 2BJ) where package will be signed for at the Reception Desk.

2.6.
Why is this data/information being shared?

To produce ID badges for BOB ICB employees.

-

How will you share it? (Consider and detail all means of sharing)

1. Digital Team to send ESR spreadsheet and pictures to ID Card Centre via secure NHSmail Egress.
2. ID Card Centre data process steps:
    - Data is downloaded and saved to the ID Card Centre Server based at HQ
    - Once on the server, the data is only accessible by specific members of the Team who have received full GDPR and information security training.
    - Once data has been printed and the cards shipped out, the data is kept on the ID Card Centre server for 30 days.
    - After the 30 days the data is purged and permanently deleted.
    - With regards to shipping the ID cards. All orders will be shipped by UPS insured service courier.
3. ID Card Centre if required, will edit pictures before producing the ID Badges for BOB ICB employees.
4. ID Card Centre to ship the orders to designated secure office location (NHS Berkshire West CCG Offices, 59 Bath Rd, Reading RG30 2BJ) where package will be signed for at the Reception Desk.

Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements ☐

Provide details of how you have considered any privacy risks of using one of these solutions
Click here to enter text.

2.7.
What data sharing agreements are or will be in place?
No. Data sharing will be based on contract exchange with ID Card Centre with DPIA as an attachment to it.

2.8.
What reports will be generated from this data/information?
Internal reports only, covering number of ID badges issued.

2.9.
Are you proposing to use Data that may have come from NHS Digital (e.g. SUS data, HES data etc.)?
No

If yes, are all the right agreements in place?
Choose an item.

Give details of the agreement that you believe covers the use of the NHSD data
Click here to enter text.

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

3.1
Are you proposing to use a third party, a data processor or a commercial system supplier?
Yes

If yes use these spaces to add their details including their official name and address. If there is more than one then include all organisations. If you don't know then stop and try and find this information before proceeding.

ID Card Centre Limited, HQ, 53 Tenter Road, Moulton Park, Northampton NN3 6AX.

Click here to enter text.
Click here to enter text.

3.2
Is each organisation involved registered with the Information Commissioner? Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Registered	Registration details or comments if not registered
BOB ICB	Yes	ZB343068
ID Card Centre	Yes	Z3192093
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

3.3
What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller? (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

ID Card Centre has provided controller with a copy of Data Protection Policy the Id Card Centre operate on please see attached

IDCC IS Data Protection Policy.pd

This policy document covers the processes and policies for data management within information security at ID Card Centre. Additionally, the NHS Contract will be exchanged with the ID Centre with the DPIA provided in the attachment to the contract.

Name of organisation	Brief description of assurances obtained
ID Card Centre GDPR regs can be found on the supplier website - https://www.idcardcentre.co.uk/gdpr	• ICO registration certificate and number - Z3192093
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

3.4

What is the status of each organisation's Data Security Protection Toolkit?

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
Buckinghamshire Oxfordshire and Berkshire West ICB	QU9	Standard Exceeded	27/06/2023
ID Card Centre	N/A		
			Click here to enter text.

3.5

How and where will the data/information be stored? (Consider your answer to 2.7 and the potential storage of data in any online meeting or networking solution).

1. Digital Team to send ESR spreadsheet and pictures to ID Card Centre via secure **NHSmail Egress**.
2. ID Card Centre data process steps:
   - Data is downloaded and saved to our Server based at HQ ID Card Centre Limited, HQ, 53 Tenter Road, Moulton Park, Northampton NN3 6AX
   - Once on our server, the data is only accessible by specific members of the Team who have received full GDPR and information security training.
   - Once data has been printed and the cards shipped out, the data is kept on Four server for 30 days, which gives you plenty of time to check the order to make sure your happy with everything.
   - After the 30 days are up and we've not received any query from the client, the data is purged and permanently deleted.

3.6

How is the data/information accessed and how will this be controlled?

- Data is downloaded and saved to the ID Card Server based at ID Card Centre Limited, HQ, 53 Tenter Road, Moulton Park, Northampton NN3 6AX
- The data is only accessible by specific members of the Team who have received full GDPR and information security training.

3.7

Is there any use of Cloud technology?

No

If yes add the details here.

Egress integrates seamlessly with Microsoft Outlook to provide one-click, easy-to-use email encryption. Open a new message in Outlook, completing the To, Cc and Subject fields. Compose your message and attach any files as normal. Outlook messages are Unclassified as default (this default can be changed where required)

3.8

What security measures will be in place to protect the data/information?

ID centre computers are password protected. All computers are kept up to date with suitable anti-virus and malware protection.

ID Card Centre has provided controller with a copy of Data Protection Policy the Id Card Centre operate on please see attached.

IDCC IS Data Protection Policy.pd

This policy document covers the processes and policies for data management within information security at ID Card Centre. Additionally, the NHS Contract will be exchanged with the ID Centre with the DPIA provided in the attachment to the contract

Is a specific System Level Security Policy needed?

No

If yes or don't know then you need to speak to your Data Protection Officer to ensure one is put in place if needed.

3.9

Is any data transferring outside of the UK? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

If yes describe where and what additional measures are or will be in place to protect the data.

3.10

What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?

ID Card Centre does not have a data processing agreement with ICB – this processing is only for purpose of printing ID card

This policy document covers the processes and policies for data management within information security at ID Card Centre. Additionally, the NHS Contract will be exchanged with the ID Centre with the DPIA provided in the attachment to the contract

4. Privacy Notice, Individual Rights, Records Management, Direct Marketing

4.1

Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date? (There is a checklist that can be used to assess the potential changes required or if you wish for it to be reviewed then add the link below).

The staff privacy notice will be updated to include use of ID badge data.

4.2

How will this activity impact on individual rights under the GDPR? (Consider the right of access, erasure, portability, restriction, profiling, automated decision making).

No impact.

4.3

How long is the data/information to be retained?

- Once data has been printed and the cards shipped out, the data is kept on Four server for 30 days, which gives you plenty of time to check the order to make sure your happy with everything.
- After the 30 days are up and we've not received any query from the client, the data is purged and permanently deleted.
- Data at ICB will be retained according to the ICB records management policy.

4.4
How will the data/information be archived?

- Once data has been printed and the cards shipped out, the data is kept on Four server for 30 days, which gives you plenty of time to check the order to make sure your happy with everything.
- After the 30 days are up and we've not received any query from the client, the data is purged and permanently deleted.
- Data will be archived according to the ICB records management policy.

4.5
What is the process for the destruction of records?

- Once data has been printed and the cards shipped out, the data is kept on Four server for 30 days, which gives you plenty of time to check the order to make sure your happy with everything.
- After the 30 days are up and we've not received any query from the client, the data is purged and permanently deleted.
- Data will be destroyed in accordance with ICB records management policy.

4.6
What will happen to the data/information if any part of your activity ends?
The ID centre to delete all the data held with them if any activity ends including any ID which will have not yet been despatched to ICB.

4.7
Will you use any data for direct marketing purposes? (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)
No

If yes please detail.
Click here to enter text.

5. Risks and Issues

5.1
What risks and issues have you identified? The DPO can provide advice to help complete this section and consider any measures to mitigate potential risks.

Describe the source of risk and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Loss of data in transfer.	Possible	Significant	High
Incorrect data on ID Badge.	Possible	Minimal	Medium
Loss of ID Badges in transit.	Possible	Significant	High
Data retained and lost / misused at ID Card Centre	Possible	Significant	High

5.2

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved (SIRO)
Loss of data in transfer (The general point with the project is that the ICB will be sending the names and pictures ('the IDs') of over one hundred employees, which is data that if not secured, could be misused / shared for fraudulent purposes)	HR/Digital Team/Employee to use secure NHSmail email addresses. Recipient email address to be used need to be name and cannot be a shared mailbox to receive data.	Reduced	Medium	Choose an item.
Incorrect data on ID Badge.	Checking data process to include both Admin and HR.	Eliminated	Low	Choose an item.
Loss of ID Badges in transit.	Use of the **UPS** Courier service. UPS Courier are an insured service, with parcel tracking and signed for postage which will be used to deliver the ID Badges to NHS secured office in Reading, Bath Road. Confirmation email that the package has been received, will be sent from the Reception staff (who signed for the package). Secured location where the package is to be kept is identified and agreed between Digital Team/HR and Reception Staff in Reading Office.	Reduced	Medium	Choose an item.
				Choose an item.
Data retained and lost / misused at ID Card Centre	Agree timescales for deletion of all data held by ID badges	Reduced	Medium	

5.3

What if anything would ?

If there is a delay in the consultation period, there is a risk that staff will leave or change roles and monies will be wasted on having to re issue ID cards.

Also if the production of accompanying policies and procedures is delayed there is a risk of Identity fraud when staff need to visit NHS locations buildings, NHS Services to carryout work or attend meetings.

Possible risk that projects could be delayed due to identity not being confirmed with Identity Card and staff not being able to access premisses to carryout essential work.

Risk of Identity fraud when staff visit NHS locations buildings. Risk of delay in the consultation process, would mean a delay in continuing with the project.

5.4
Please include any additional comments that do not fit elsewhere in the DPIA?
None

6. Consultation

6.1
Have you consulted with any external organisation about this DPIA?
No

If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.
Because of the small scale of the project.

6.2
Will you need to discuss the DPIA or the processing with the Information Commissioners Office? (You may need the help of your DPO with this)
No

If yes, explain why you have come to this conclusion.

7. Data Protection Officer Comments and Observations

7.1 Comments/observations/specific issues	Click here to enter text.

8. Review and Outcome

Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:
A) There are no further actions needed and we can proceed

If you have selected item B), C) or D) then please add comments as to why you made that selection
Click here to enter text.

We believe there are
Choose an item.

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures you could take and include these in the green boxes below

Residual risks and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved (SIRO)**
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Signed and approved on behalf of Buckinghamshire Oxfordshire and Berkshire West Integrated Care Board

Name: [redacted]

Job Title: Data Protection Officer

Signature: [redacted] Date: 26/07/2023

Signed and approved on behalf of Click here to enter text.

Name: Click here to enter text.

Job Title: Click here to enter text.

Signature: Click here to enter text. Date: Click here to enter a date.

Please note:

You should ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant.

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here:
Click here to enter text.