NHS
East London
NHS Foundation Trust

Data Protection Impact Assessment (DPIA)
Template

A Data Protection Impact Assessment (DPIA) must be completed whenever a new service, process or information asset is introduced or there is a change to an existing process or service. Steps 1 – 3 must be completed for all projects / proposals. If advised to do at the end of Step 3 please complete Step 4. Completed DPIAs should be emailed to [redacted].

Step 1. Project / proposal details *Complete for all projects / proposals*

Project / proposal name:

Project: Body Worn Cameras

Purpose: Aid the role of staff and team communication in reducing seclusion, restraint and forced tranquilisation in acute inpatient mental health settings

Description of project / proposal: Explain broadly what project aims to achieve and what type of processing it involves. Please attach a document or link to other documents, such as a project proposal if you have one. Is it a new electronic system, service acquisition, software, information sharing proposal or something else?

The body worn cameras are being implemented on two acute inpatient mental health wards [redacted] as part of an National Institute for Health Research – Research for Patient Benefit funded study titled: '*The Role of Staff and Team Communication in Reducing Seclusion, Restraint and Forced Tranquilisation in Acute Inpatient Mental Health Settings*' (see link to study: NIHR Funding and Awards Search Website).

The research study protocol is attached. This study has been reviewed, approved and given a favourable opinion by an independent NHS research ethics committee, Wales REC 3. All costs associated with the introduction of the cameras on wards will be met by the NIHR RfPB grant.

Why are we doing this research?
Over 100,000 patients are admitted to acute mental health wards annually, 40% involuntarily. Wards are under incredible pressure due to high bed occupancy rates and staff shortages. In England, 80% of nurses report experiencing patient aggression. Staff manage patient aggression using communication, known as de-escalation. However, one in three de-escalations are unsuccessful and staff use restrictive practices including: restraint, seclusion and forced tranquilisation. In England 60,000 restraints occur annually, leading to patient harm (even death), trauma, fear and feelings of being disempowered and dehumanised. Staff experience harm, anxiety and burn out. De-escalation practice varies and training is not evidence based. Communication is clearly important in de-escalation but we don't know what communication is effective.

Research aims and anticipated outcomes?
The overall aim of this research study is to identify the communication that characterises successful de-escalation of patients displaying aggressive behaviour in acute mental health settings, avoiding the need to use physical restraint (held to prevent movement), seclusion (locked in isolation) and forced tranquilisation (involuntarily injected with psychotropic medication). This can only be

achieved through detailed analysis of staff and team communication. It is for this reason that we are proposing recording staff communication using body worn cameras. Similar cameras are already in place in other mental health trusts within the UK (e.g. West London NHS Trust).

This is solely a research project, the results of this project will be used to inform the staff training. Redacted video footage may be used for educational training but only with explicit consent from all participants in the video.
This study will generate much needed empirical evidence to inform professional training of clinical staff in de-escalation and aggression management. Collaborations with educational partners will speed the translation of these findings into practice, improving patient care, staff wellbeing and overall safety.

The Body Worn Cameras
The cameras are being supplied by a company called Reliance, who provide secure body worn cameras to the police and healthcare trusts. This is a new process that is being implemented as part of this research study.
The purpose of the research study is to conduct a detailed examination of staff communication on mental health wards, specifically at times when patients are displaying challenging behaviour. Analysis of communication at this level of detail requires audio-video recorded interactions. Body worn cameras, similar to those used in other mental health trusts within the UK were seen as the most appropriate way to record such interactions for the following reasons:

- They do not record continuously but can be switched on and off easily by staff.
- They are completely secure
- They have been used successfully in other mental health trusts within the UK.
- They have actually been shown to reduce violence, staff complaints and restraints in other mental health trusts within the UK (Elis et al., 2019; Hardy et al., 2017)

Give an overview of the processing: How will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? Attach a flow diagram or describe data flows. What types of processing identified as likely high risk are involved?

Data will be collected on two different Acute mental health inpatient Wards [redacted]. Each ward will be equipped with 5 body worn cameras worn by staff and one body worn camera will be used by a researcher on both wards. The researcher does not need to be present when de—escalation takes place. Should a de-escalation episode happen while the researcher is on the ward, the researcher will have the opportunity to record it as well. The main purpose of the researcher on the ward is to complete ethnography observations and to consent participants.
Cameras will be activated when staff and/or researcher feel a de-escalation intervention is likely to happen (i.e. the service user is displaying challenging behaviour). Staff are to advise the patient that they are going to start recording.
Data, in the form of integrated video and audio footage, will be used to analyse verbal and non-verbal communication during de-escalation interventions for the purpose of the research study and will not be shared outside of this project (ELFT, Reliance approved staff members, the researchers and management.)

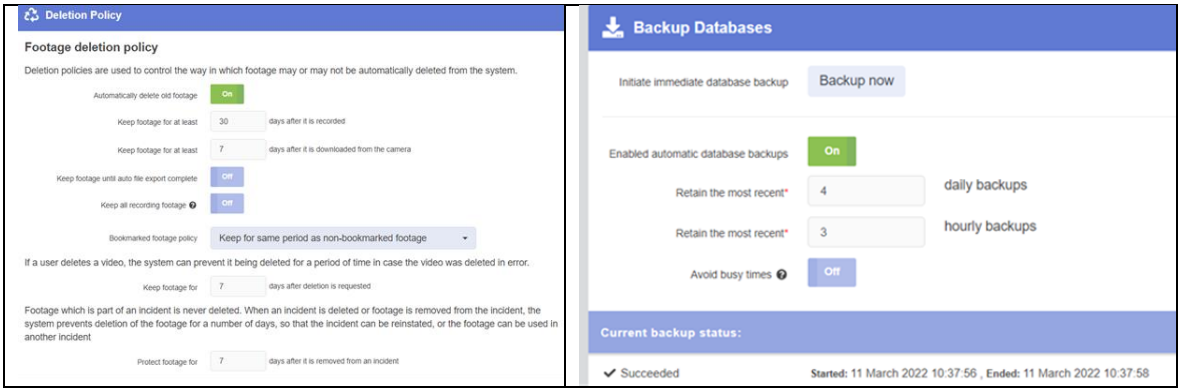
- Recordings will be stored on Reliance secure servers for 30 days and will automatically be deleted after this time unless a request is raised by the trust to extend this period in order to include the footage in the study (Max 99 years)

- Recordings that are being included in the study will be stored for 20 years in line with the Department of Health NHS Code of Practice on Records Management all video recordings.
- Recordings will contain no patient identifiers, although participants (patients and staff) will be visible in the footage.
- Staff will explicitly state that they are "*turning on the camera*" before any recording starts to inform others. Patients who are not related to the incident will be blurred from the recordings. No names, patient data, patient identifiers will be captured or stored. Audio & Video will not leave the trust and will remain in the Trusts secure AWS environment.
- Patients will only be informed that the recording is taking place according to UK GDPR guidelines, informed consent will be sought at a later stage before utilising the footage for the study.
- Where a patient does not provide consent, the recording will be deleted from the system following the process defined below.
- Recordings will be uploaded to the cloud once the camera is placed back onto the docking station. (Process flow attached below).
- We aim to approach patients for consent within 7 days of their recorded incident. This will be the case with the majority of patients. However, we will take advice from the ward lead and if they do not feel it is appropriate to approach a specific patient during this time we may need to wait and approach them at a later point, up to a maximum of 30 days. Footage will be deleted if patients are not approached within 30 days of the recording.
- To provide the rationale for this decision - obtaining consent from patients for each recording prior to the recording happening would be impractical and unethical for the following reasons:
    - We cannot consent participant to a study that they may never be part of – i.e. they may never be recorded during a de-escalation.
    - We cannot target participants who have the potential to be aggressive and consent them to a study on the basis they might display aggressive behaviour in future.
    - We cannot request consent from patients at the time of a de-escalation, as they are in a heightened state of arousal and it is a sensitive juncture in the patients care.
- Thus, it has been decided that the best option is to request consent retrospectively, which is also the standard procedure in other research sites. Patients will however know that the research is taking place on the wards and that the cameras are in use. They will be told that the camera is being switched on by staff. Patient and staff safety take priority in all situations so if a patient requests for the camera to be turned off staff are free to do this. It is up to the individual member of staff in each situation to use their own clinical judgement.

Video Deletion Process

- The first stage is that footage is deleted from VideoManager, either via the retention engine which is default set to 30 days, or manually by users with the permission to do so.
- Note, footage that forms part of Incidents on VideoManager are kept on the system until manually deleted by users with the permission to do so.
- When video is deleted by the retention engine, it is fully removed from the live database but not from backups.
- When video is deleted manually by users, the video is removed from the live view on VideoManager but sits in a 'recycle bin' for a set number of days (default is 7 days but can be configured) before being removed from the live database but not from backups. This is a safety step to recover video if it is accidentally deleted.

- The backups are performed hourly and daily. These can also be configured but the default is 3 hourly backups and last 4 days backups.
- These backups are disaster recovery options only. The whole customer platform is backed up, not individual video files.
- So, for full removal of a video file using the platform default settings:
    - Retention engine deletion day 1 to remove from live database – day 1
    - For manually deleted video files there is a further 7 days in 'recycle bin' to remove from live database – day 7
    - Last backup containing that video file is deleted 4 days later – day 11
    - Maximum 11 days to delete from live database and backups.



Is a supplier involved in the processing? If the supplier is known at this stage, give supplier details – attach evidence of DSPT accreditation, BS27001 accreditation or otherwise copies of their information security policies, evidence of IG training etc

[redacted]

Reliance hold both ISO27001 and Cyber Essentials Certifications. The data is held with the London AWS data centre. Backups are held in the AWS EU datacentre split across Germany and Ireland.

What are the benefits?

The research study that requires the use of the body worn cameras is funded by the Research for Patient Benefit stream of the NIHR funding scheme. The overarching aim of this study is to improve patient care. At the end of this 24-month study, our analysis of the body worn camera footage will have identified the communication that characterises successful de-escalation of patients displaying aggressive behaviour in acute mental health settings. This will provide the first empirical evidence that can be used to inform staff training. This training will be disseminated to participating wards and the ELFT trust more widely by the end of the study (approx.. Jan 2024). By improving de-escalation practice the reliance on use of potentially harmful (for patients and staff) restrictive practices (e.g. restraint, seclusion, forced tranquilisation) can be reduced.

In the shorter term, the introduction of body worn cameras (BWC) may also improve staff and patient safety. Other trusts have reported a reduction in patient violence and staff complaints following implementation of BWCs (Elis et al., 2019; Hardy et al., 2017).
Proposed implementation date: April 1st to 31st December 2022

Step 2. Contact details *Complete for all projects / proposals. Please contact the IG team if anything is unclear*

Work stream lead / project manager details	
[redacted]	[redacted]
[redacted]	[redacted]
Information Asset Owner (if different from above). This will be a Service Director, Corporate Director / Associate Director	
[redacted]	[redacted]
[redacted]	[redacted]
Information Asset Administrator (or System Owner). This will usually be a team manager, IT super user etc	
[redacted]	[redacted]
[redacted]	[redacted]
Executive Director sponsor details. Required for large scale change, acquisitions etc, not for small projects	
Name: [redacted]	[redacted]
[redacted]	[redacted]

Step 3. Screening questions. *Complete for all projects / proposals*

Answering YES to any of the screening questions represents a potential high risk to the rights and freedoms of individuals and therefore a full DPIA must be completed to ensure those risks are identified, assessed and fully mitigated.

Screening questions	Yes or No
Will the project / proposal involve the collection / processing of information about individuals? (this could be service users, carers, staff, stakeholders etc)	**Yes**
Does it introduce new or additional information technologies that can substantially reveal business sensitive information / have a high impact on the business?	**Yes**
Will it require individuals to provide information about themselves?	**No**
Will information about individuals be disclosed to organisations / individuals who have not previously had routine access to the information?	**Yes**
Will information about individuals be used for a new purpose or in a new way?	**Yes**
Does it use technology that could be seen as intrusive e.g. automated decision making?	**No**
Will it result in making decisions about individuals that may have an impact on them e.g. research, service planning, commissioning new services?	**Yes**
Will it change the delivery of an individual's direct care?	**No**
Will it require you to contact individuals in a way they might find intrusive?	**No**
Does it involve any other organisations?	**Yes**
Does it require individuals to consent to their information being processed?	**Yes**
Does it involve new or significantly changed handling of a considerable amount of personal / business sensitive information about an individual in a database or system?	**Yes**
Does it involve new or significantly changed consolidation, interlinking, cross referencing, or matching of personal / business sensitive data?	**Yes**
Does it use cloud services / is it stored in 'the cloud'?	**Yes**
Is it about children or vulnerable groups of adults e.g. service users?	**Yes**
Will it be used for research purposes / projects?	**Yes**

If you answered YES to any of the above questions please complete Step 4. If you answered NO to all questions then please send your DPIA [redacted] We will assess your request and either confirm our data protection support for your project / proposal or request further information. Please contact the IG team if anything is unclear.

Step 4. Full Data Protection Impact Assessment *Complete only when advised a full DPIA is necessary at the end of Step 3*

4.1 Processing
What data will be collected / processed? Does it include health or any other special categories of data? If so, please list. These are health, racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation This study will involve observations of routine working by a researcher through ethnographic observations carried out in person to identify and analyse unexpected issues. Observation of routine working will be obtained by conducting ethnography observations on the wards, in other words, the study researcher will spend time shadowing staff and having brief discussions with them about their work in-situ. Observations will be documented as field notes. This will take place on acute mental health inpatient wards and will be supported by video footage of mental health staff interacting with patients. Patients' notes will be looked at by members of the research team to understand patient's history of violence and diagnosis, but identifiable information will not be stored. Whilst no identifiable information is collected from the patient (e.g. hospital number and date of birth) in order to conduct the research, we need to request consent from patients for analysis of their video footage. We also need to extract from their notes their previous history of violence, diagnosis and current mental state. We are collecting these factors because of their role in aggression management. This information is pseudonymised.
How will the data be collected? Body worn cameras will be worn by mental health staff in inpatient acute wards. Cameras will not be recording constantly but will only be turned on by staff when they feel they are de-escalating a patient that is displaying challenging behaviour. The staff member will inform the patient when they are about to start recording. Recorded incidents will only be included in the study and analysed if all parties involved provide informed consent to participate. If patients lack capacity to provide informed consent their footage cannot be included in the study. Senior staff on the ward will inform the research team which patient have provided consent. There are multiple level of consent in this study. Firstly ward leads will consent to the research taking place on their ward and for cameras to be implemented. Secondly, ward staff will consent to recording footage during their shifts. Thirdly, once eligible footage has been identified for potential inclusion in the study, we will then approach the patients involved for their consent to use this footage. Therefore, we do not require patient's consent for the recording to happen, but we do require their consent for their footage to be used as part of the research.
Where will it be collected from? Acute adult inpatient mental health wards [redacted]
What will it be used for?

For research purposes only.
Although the funding has been awarded for the research project, it is possible that this work will also feed into quality improvements within the Trust.

Will it be processed manually? Yes

Yes. Although the recorded footage will be collected and uploaded to the secure server automatically, identification of footage for inclusion in the study and subsequent analysis will be conducted manually.

Will it be processed electronically? Yes or No

Yes

How is access controlled? For example, passwords, Smartcard, locked door

Only members of the direct research team will have access to the system where the data will be based. This will be controlled using Username and passwords. This includes 2 approved contacts from Reliance

Will only the minimum data necessary be collected / stored / processed?

Yes, data will be deleted if it is not part of the study after 30 days.

Footage that has been included in the study will be retained for 20 years in line with requests from Research Ethics.

Will be anonymised, pseudonymised or collated with other data?

The footage will be pseudonymised and collated with sociodemographic data (i.e. history of violence, number of previous admissions) but not identifiable information.

Footage will only be used where patients have been selected for inclusion in the study and have provided informed consent.

Will any third parties access the data? Who? For example if another organisation wants access to our systems
Yes, Reliance – for system support only.

Will it be sent off site or shared externally i.e outside the Trust or outside its computer network? Yes or No

Yes, footage will be accessible by approved candidates outside of trust. The data will not be stored on the Trust network at any stage.

If sent off site, where to? Name the other agency / company / location / country

Reliance (AWS – London, Ireland and Europe) Recordings that are part of the study will be stored securely in a password protected server at the collaborator City, University of London for analysis. This has been checked from a security and data protection standpoint.
If so, is there a contract / data controller to processor agreement, information sharing agreement? If yes, please attach Yes, [redacted]
How will it be sent? [redacted]
How long will the data be retained in identifiable form? Only recorded footage that has consent from both staff and patients involved will be included in the study and retained. All other footage collected will be deleted automatically 30 days after recording. Footage that has been included in the study will be retained for 20 years in line with requests from Research Ethics.
Will it be de-identified or destroyed. How? Data not included in the study will be deleted from the portal.
Are you aware of any concerns or risks over the processing / use of the data, system, supplier, other agency etc? No
Has any / will any consultation take place? Yes or No? Please list, also include feedback received Yes. The research team and ELFT leads are currently engaging with ward staff to discuss any concerns or questions they may have about the introduction of the cameras and the research study more generally. Overall the evidence suggests that the implantation of body worn cameras on mental health wards may have the potential to improve patient and staff safety. Staff are understandably curious about the use of cameras on wards as this is a new avenue for the teams involved. We have set up a robust multi-level consent process as part of this study to ensure that staff and patients are comfortable with the data we collect. Staff may consent to participate in the study and record their interactions with patients but they will have the option to ask for any footage recorded to be removed from the study if they wish. They will also have the option to review their own footage at any time (see protocol for more details).

Only recorded footage that has consent from both staff and patients involved will be included in the study and retained for 20 years. All other footage collected will be deleted automatically 30 days after recording.

4.2 Additional Information

- Recordings will be uploaded securely as soon as a device is replaced on the docking station, typically at the end of the shift.
- Video will remain in the cloud for 30 days at which point it will be included in the study (providing consent has been provided) or deleted automatically. Deleted video will be sent to bin for 7 days after which the video cannot be restored.
- Video's will be blurred to protect people who have not provided consent to the study.
- The Redacted file will be exported for storage if it is selected for the study. Redacted recordings will be exported to city server prior to analysis. Video can be stored for up to 20 years in line with ethics.
- Users can withdraw their consent from the study at any time, however video that is captured prior to the removal of consent will remain part of the study. Users who decided to opt against being in the study will not be asked to participate in this study later.
- All body worn camera wearers will have control over what is being recorded. Only researchers, managers and approved Reliance staff members will have access to the recording footage.
- Cameras will only to be used in the event of de-escalation.
- Users will be required to sign in/out the devices at the start and end of their shift.
- Users must announce that they are turning on the camera before starting the recording.
- Cameras must be placed on the docking station to upload footage and recharge.
- Users will be advised to end the recording once the situation has passed.
- Consent approval for the use of cameras will be reactive.

4.3 Cloud considerations. You must complete this if you answered Yes in Step 2 to 'Does it use cloud services / is it stored in 'the cloud'?
Which country is the cloud provider based in? Amazon Web Server (AWS) in London – Backup data centres in Ireland and Germany – Security document attached above.
Is the cloud service hosted on HSCN? No
What business continuity plans are in place if the provider ceases trading? The study will only take place in 24-month period so the risk is greatly reduced. However, we will seek alternative providers if this was to happen.
What secure arrangements are in place at the end of the contract with the cloud provider to transfer the data? Exporting Available
Who would legally own any data uploaded to the cloud application by the Trust? ELFT
What information & cyber security policies does the cloud provider have? Please attach information / embed a link ISO27001 and Cyber Essentials – Security document attached above.
The above has been reviewed by [redacted]. They have advised that they are happy to test the equipment but will not officially commence until this document has been approved. The digital team are also aware of this project as they are kept up to speed via our weekly checkpoint meetings.

Please send your completed DPIA [redacted] We will assess your request and either confirm our data protection support for your project / proposal or request further information.

Information Governance assessment

To be completed by the information governance team who will advise you once the assessment is complete

Compliance area	**Assessment of compliance**	**Compliance agreed by IG Manager Y / N**
Principle 1 Lawfulness, fairness and transparency Transparency: Are data subjects aware what data processing will be done? Fair: Is the processing as described? Lawful: Processing must meet the tests described in GDPR [article 5, clause 1(a)], that personal data shall be: "(a) processed lawfully, fairly and in a transparent manner in relation to individuals	. Service users will be made aware that they are recorded. Consent to use the data will be sought prior to using recordings for the study. It is fairly processed under Article 6 (e) Public Task, and Article 9(2)(h) GDPR (health or social care with a basis in law) read with Schedule 1 paragraph 2 of the Data Protection Act 2018.	**Y**
Principle 2 Personal data can only be obtained for "specified, explicit and legitimate purposes" [article 5, clause 1(b)]. Is the data only being used for the specific processing purpose that the subject has been made aware of?	Cameras are turned on and record once de-escalation is to be used. Camera are not continually recording.	**Y**
Principle 3 Data collected on a subject should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [article 5, clause 1(c)]. Is only the minimum amount of data kept for specific processing?	Cameras are turned on and record once de-escalation is to be used. Cameras are not continually recording and patients are made aware that data may be retained if they consent to the study as stated in their Patient Information Survey (PIS).	**Y**

Principle 4 Personal data shall be accurate and, where necessary, kept up to date. [article 5, clause 1(d)]. Baselining ensures good protection and protection against identity theft. Are there rectification processes in the data management / archiving activities	Camera are not continually recording. Only service users showing aggression and noted for de-escalation will be recorded.	**Y**
Principle 5 Regulator expects personal data is "kept in a form which permits identification of data subjects for no longer than necessary" [article 5, clause 1(e)]. Is this recognised and what processes are in place to ensure it happens?	Data will be deleted if not part of the study after 30 days. Data will be deleted immediately if service user does not consent to be part of the study. Footage that has been included in the study will be retained for 20 years in line with requests from Research Ethics	**Y**
Principle 6 Requires processors to handle data "in a manner [ensuring] appropriate security of the personal data including protection against unlawful processing or accidental loss, destruction or damage" [article 5, clause 1(f)]. Is the security adequate? Is there a system level security policy?	Data is accessed by members of the research team who will have access via a username and passwords. The footage cannot be removed from the camera and will only be uploaded to the secure server when the camera is replaced on the dock. There is no other means to gain access to the footage.	**Y**
Information sharing Is an information sharing or third party access agreement required? Y/N	N	**Y**
Cloud considerations Has the Information Security Manager	Yes	**Y**

<table>
<tr><td>approved the Cloud section? Y/N</td><td></td><td></td></tr>
<tr><td>Risks
Assess the source of risk & nature of potential impact on the rights & freedoms of individuals. Include associated compliance & corporate risks as necessary</td><td>
<table>
<tr><td></td><td colspan="5">Likelihood</td></tr>
<tr><td>Severity</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
<tr><td></td><td>Rare</td><td>Unlikely</td><td>Possible</td><td>Likely</td><td>Almost</td></tr>
<tr><td>5 Catastrophic</td><td>5</td><td>10</td><td>15</td><td>20</td><td>25</td></tr>
<tr><td>4 Major</td><td>4</td><td>8</td><td>12</td><td>16</td><td>20</td></tr>
<tr><td>3 Moderate</td><td>3</td><td>6</td><td>9</td><td>12</td><td>15</td></tr>
<tr><td>2 Minor</td><td>2</td><td>4</td><td>6</td><td>8</td><td>10</td></tr>
<tr><td>1 Negligible</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td></tr>
</table>

Unlikely = 2 x Minor = 2
Total Risk = 4

Is the risk great enough to report to the ICO?

No

Add comments:

Cameras are not continuously recording. Consent sought to record prior to cameras being turned on.
</td><td></td></tr>
<tr><td>Asset register / data flows mapping
Has the asset been added to the relevant asset register? Y/N</td><td>All devices will be included on the asset register and will be tracked as and when a device allocated to a member of staff.</td><td><u>Y</u></td></tr>
</table>

Information governance team to forward to DPO

Data Protection Officer Approval

DPO comments
Approved provided there is clear signage advising the purpose of the recording, that recording may take place during escalation and that consent for retention of recordings will be sought after the event. Service users should also be advised on admittance they have the option to dissent generally from being filmed during de-escalation provided this is documented during the admittance process.
DPO approval granted? Y/N Yes

DPO name: [redacted]
DPO signature: 
DPO approval date: 08/06/2022

DPO to return form to information governance team for documenting and returning to project manager

Date returned by IG team to project manager: **09/06/2022**