**Parish CCTV Assessment**

**Introduction:**

This assessment will help you to assess the risks, to ensure that you understand your responsibilities

and that you have a record of your decision-making. The Diocese of Westminster (the Data Controller) is registered with the Information Commissioners Office (ICO) and therefore parishes are not required to register their use of CCTV with the ICO.

Before you undertake the completion of this assessment, it would be beneficial to you to refer to the CCTV in Parishes guidance, **Appendix 1** and the Guiding Principles, **Appendix 2**

Appendices 3, 4 and 5 are for you to customise, should you wish to, but keeping the contents as they are and printing them as required.

The completed CCTV assessment, together with the logs should be kept in your physical Data Protection file, together with your Parish data processing record, confidentiality agreements and parish computer codes of practice.

Please review this assessment annually or when any changes are made to your CCTV system. Changes made to the CCTV system after it has been initially signed off by the Data Protection Officer (DPO) must be notified to the DPO.

**Contents:**

Introduction & contents Page 1

CCTV Assessment Pages 2 – 8

Changes to CCTV system Page 9

Appendix 1 – Guidance for CCTV in Church premises Pages 10 – 12

Appendix 2 – Guiding principles Page 13

Appendix 3 – CCTV camera location log Page 14

Appendix 4 – CCTV functionality log Page 15

Appendix 5 – CCTV incident log Pages 16 – 17

**Parish CCTV Assessment**

**Please do NOT include anything on the form that relates to livestreaming of events**

|  |  |
| --- | --- |
| **Parish name/Area:** |  |

|  |
| --- |
|  **Section 1: Identify the need for your CCTV (*you may tick more than 1 box*)** |

 Protection & detection of crime Safety of staff, volunteers & visitors

□ Deterring vandalism/ damage to property □ Anti-social behaviour

□ To ensure the safety of the church when it is kept open during the day

□ Other . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Please state reasons for the installation of CCTV and any consultations you have undertaken, e.g. parish meetings, meeting with police, insurers etc. Previous documented incidents should be kept securely with this assessment. You may attach supporting documents of consultations held.

|  |
| --- |
|  |

|  |
| --- |
| **SECTION 2: Consider necessity and proportionality. What is your lawful basis for using the CCTV? (*you may tick more than 1 box*)** |

Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider potential Safeguarding issues and discuss this with your PSR or the Safeguarding department.

 Public Interest Legitimate Interest □ Other . . . . . . . . . . . . . . . . . . . . . . . . .

|  |
| --- |
|  |

|  |
| --- |
| **SECTION 3: What other less intrusive solutions have been considered?** |

You need to consider other options prior to using CCTV. (continue on a separate sheet if necessary).

|  |
| --- |
|  |

**Signage (*you may tick more than one box*)**

How will you inform people that they are under surveillance and ensure their privacy is maintained? Consider whether data subjects would reasonably expect to be under surveillance in this context.

□ Appropriate signage □ Informed verbally e.g. counters

□ Other (please specify) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .



Example of a sign to use

inside buildings (approx.. 4” x 4”):

Please see page 3 of Appendix 1 of a sample sign to be used externally, e.g. the car park.

The Data Controller is The Diocese of Westminster and the contact details (email/phone) should be that of the parish.

Complete the CCTV Camera Location Log, **Appendix 3**.

**Retention and Deletion of CCTV images**

Does the system’s technology enable recording? □ Yes □ No

Is audio being recorded? (other than livestreaming) □ Yes □ No

If recording is enabled, please state how?

□ Parish hard drive □Tapes/disks etc. □ Contractor’s Server\*

□ Other (please specify) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Does the service contractor monitor your CCTV for the parish? □ Yes\* □ No

 *\** Attach a copy of the contract with this assessment

The quality and functionality of the CCTV will be checked:

□Weekly□ Monthly □ Other . . . . . . . . . . . . . . . . .

Ensure that the Parish CCTV Functionality Log, **Appendix 4**, is completed. This will be audited by the Parish Support Team.

**Security Measures**

Is the monitor out of sight, i.e. only available to those authorised to view the images?

□Yes□ No

Are the CCTV images available on any other device?

□Mobile phone□ PC/laptop □ Tablet

□ Other device (please specify) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Who has access to the visual data? . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

How long is the data held for before being overwritten? . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Do you have written instructions on downloading the required CCTV footage?

□Yes□ No Please attach the instructions to this assessment

Record any incidents captured on the Parish CCTV Incident Log and keep these securely in your Data Protection folder, **Appendix 5.**

Who are the administrator(s) of the CCTV? . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Has the CCTV policy and training been provided to them? . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**Responding to requests of CCTV footage: Contact the DPO in the first instance (tel.: 0207 798 9015 or email dpo@rcdow.org.uk)**

|  |
| --- |
| **SECTION 6: Identify the risks** |

Identify and evaluate the risks to the rights and freedoms of individuals relating to the CCTV system. Could it interfere with other rights and freedoms such as those of conscience and religion, expression or association?

**Describe source of risk and nature of potential impact on individuals.** Include associated compliance and corporate risks as necessary.

Risk 1.

|  |
| --- |
|  |
| **Likelihood of harm***(Remote, Possible or, Probable)* | **Severity of harm***(Minimal, Significant or Severe)* | **Overall risk***(Low, Medium or High)* |
|  |  |  |

Risk 2.

|  |
| --- |
|  |
| **Likelihood of harm***(Remote, Possible or, Probable)* | **Severity of harm***(Minimal, Significant or Severe)* | **Overall risk***(Low, Medium or High)* |
|  |  |  |

Risk 3.

|  |
| --- |
|  |
| **Likelihood of harm***(Remote, Possible or, Probable)* | **Severity of harm***(Minimal, Significant or Severe)* | **Overall risk***(Low, Medium or High)* |
|  |  |  |

Risk 4.

|  |
| --- |
|  |
| **Likelihood of harm***(Remote, Possible or, Probable)* | **Severity of harm***(Minimal, Significant or Severe)* | **Overall risk***(Low, Medium or High)* |
|  |  |  |

Continue on a separate page if needed.

|  |
| --- |
| **SECTION 7: Address the risks** |

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. What security features, safeguards and training will be in place to reduce any risks to data subjects?

**Identify additional measures you could take to reduce or eliminate risks identified below:**

Risk 1.

|  |
| --- |
|  |
| **Options to reduce or eliminate risk: EFFECT ON RISK***(Eliminated, Reduced or Accepted)* | **Options to reduce or eliminate risk: RESIDUAL RISK***(Low, Medium or High)* | **Options to reduce or eliminate risk: MEASURE APPROVED***DPO to complete (Yes or No)* |
|  |  |  |

Risk 2.

|  |
| --- |
|  |
| **Options to reduce or eliminate risk: EFFECT ON RISK***(Eliminated, Reduced or Accepted)* | **Options to reduce or eliminate risk: RESIDUAL RISK***(Low, Medium or High)* | **Options to reduce or eliminate risk: MEASURE APPROVED***DPO to complete (Yes or No)* |
|  |  |  |

Risk 3.

|  |
| --- |
|  |
| **Options to reduce or eliminate risk: EFFECT ON RISK***(Eliminated, Reduced or Accepted)* | **Options to reduce or eliminate risk: RESIDUAL RISK***(Low, Medium or High)* | **Options to reduce or eliminate risk: MEASURE APPROVED***DPO to complete (Yes or No)* |
|  |  |  |

Risk 4.

|  |
| --- |
|  |
| **Options to reduce or eliminate risk: EFFECT ON RISK***(Eliminated, Reduced or Accepted)* | **Options to reduce or eliminate risk: RESIDUAL RISK***(Low, Medium or High)* | **Options to reduce or eliminate risk: MEASURE APPROVED***DPO to complete (Yes or No)* |
|  |  |  |

Continue on a separate page if needed.

**Any other comments about the CCTV**

Assessment completed by, Full name: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Position held: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . *(if not Parish priest, but authorised to complete on his behalf)*

Signature: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . Date: . . . . . . . . . . . . . . . . . . . . . . . .

Name of Parish Priest: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . Signature: . . . . . . . . . . . . . . . . . . . . .

**DPO Comments:**

Signature: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . Date: . . . . . . . . . . . . . . . . . . . . . . . .

Edn. Jan. 2023

Changes made to CCTV system

|  |  |
| --- | --- |
| **Date**  | **Amendments/changes made to CCTV system** |
| Select date | Initial review |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |
| Select date | Enter text. |

**Appendix 1 Guidance for CCTV on Church Premises**

**FROM THE INFORMATION COMMISSIONER’S OFFICE (ICO) WEBSITE:**

*“The UK is recognised as a leading user of CCTV and the public are used to seeing CCTV cameras on virtually every high street. Such systems continue to enjoy general public support but they do involve intrusion into the lives of ordinary people as they go about their day-to-day business and can raise wider privacy concerns…. Images of people are covered by the Data Protection Act (DPA), and so is information about people which is derived from images – for example, vehicle registration numbers. Most uses of CCTV by organisations or businesses will be covered by the Act, regardless of the number of cameras or how sophisticated the equipment is.”*

Although the DPA already covers aspects of CCTV usage, the new GDPR also reaffirms and ‘raises the bar’ regarding the need to ensure that the processing of personal data is *lawful, fair and transparent*. As CCTV collects personal data in the form of images, it is covered by the act. In most cases, businesses and other organizations can rely on ‘legitimate interests’ and the ‘protection of persons and property’ for their legal operation of CCTV. However, they may be required to justify this against the actual day-to-day operation of the system, for example the area of coverage and where cameras are directed. Data subject's rights and freedoms cannot be overridden.

Data subjects are entitled to understand when their personal data is being processed, covering the transparency aspect of processing. It is strongly recommended that the use of CCTV be communicated via clear signage that indicates the reason why CCTV is installed, the name of the data controller and contact information in case of queries. In a church in our diocese, it is the Diocese itself (i.e. the Diocesan Trust), which is the legal entity responsible for CCTV, though the contact person will usually be the end user (e.g. local parish).

One of the core principles of the GDPR is a requirement that personal data is processed for only as long as its purpose requires it to be. The overall purpose of the CCTV system (and Possibley each camera) will need to be assessed to determine how long footage should be retained for. There are no defined acceptable retention times as it is subjective to the purpose, however be aware that several years’ later, or until new footage overwrites the old (unless this is known and quantified), is not of itself a good demonstration towards consideration of the data subjects’ rights.

As with any other aspect of personal data, data subjects have a right to access, which could result in you disclosing footage to them. CCTV operators need to ensure that the requester is present in the footage and that by supplying the footage they do not disclose any personal data of another data subject. This may involve blurring parts of the footage such as faces or car registration plates. In addition, the ICO previously recommended that subject access request of CCTV could carry an administrative fee of up to £10; this is no longer the case under the GDPR.

Security of the images (either monitored on-screen or stored on a hard drive) is essential. Any act of storage or access is considered ‘processing’ and it is imperative CCTV operators uphold the confidentiality and integrity of any footage. Screens displaying live or recorded footage should only be viewed by authorised individuals, and not by members of the public who stray past a CCTV monitor (with the exception perhaps of monitors in public areas showing footage of that area to prove to visitors that a working CCTV system is in operation). Footage should be secured, regardless of its format, for example in electronic format it should ideally be encrypted, and in physical format be locked away.

Please note that the ICO makes it clear, that with only a few very limited exceptions, conversations between members of the public should not be recorded on CCTV.

**PRACTICAL CONSIDERATIONS**

Is CCTV the right solution for the problem? – The UK is the ‘most watched’ nation with around six million cameras. Whilst people are used to this level of surveillance, many object to its continued proliferation, especially as cameras and data storage become cheaper and easier to use. If, for example, we are seeking to protect a corridor from public access, would a simple alarm system be better? If there were a problem with young people in the church grounds at night, would external lighting do the job? Is CCTV a proportional response?

What is the legal reason for retaining personal data if we record images? A supermarket might be seeking to protect stock from shoplifters, a car park operator might check registration numbers as vehicles come in and leave, a bar manager might be watching employees as they use the till – all are different legitimate reasons for using a CCTV system. A parish priest might simply want to use CCTV to keep his un-staffed church open throughout the day; but this of itself is not really a legal basis for retaining personal data. The truth is that he probably fearful of: solo worshippers Possibley being attacked, vandalism, theft or arson, and wants high-visibility cameras (even perhaps a few fake ones) to be a deterrent to would-be wrongdoers. Therefore, the legal basis for the retention of images from a church CCTV system might better described as: ‘the safety of visitors, the protection of property, and crime prevention’.

Does our CCTV usage match our stated aims? It follows that we need to be able to justify our use of a CCTV system against our stated aims. Is each camera necessary and does it actually serve our stated purposes; and are we monitoring the right areas? For example, if the aim of having a CCTV system is simply to keep an un-staffed church open throughout the day for private prayer and visitors, do we need a camera outside watching the carpark?

The quality of recorded data should also be such that it complies with your stated aims, e.g. footage for the purposes of crime prevention needs to be admissible evidence in court.

As a rule, CCTV should not be routinely monitoring ‘public’ areas outside the boundaries of your premises, e.g. a street; nor should it monitor, even partially, other private property, such as a neighbour’s garden.

A ‘privacy impact assessment’ should be undertaken before a system is installed (or retrospectively if one is not on record), and this should be reviewed annually along with policies on the storage of personal data. A Possiblee result of this might be that a particular parish decides to monitor only the church entrance and specific ‘hot-spots’, such as candle boxes, rather than have sweeping views of congregational seating which would capture people at prayer or grieving at a funeral service. Sometimes cameras can be physically switched-off for a church service, or on modern systems, pre-set to monitor only at certain times.

How long should be keep images? Most modern systems have a hard disk installed that automatically over-writes itself, thus meaning that images are not kept indefinitely. However, the storage capacity of some systems is very large, and data could be kept for up to a year. It is unlikely that most churches would need images for more than a few months to serve its legitimate purposes.

Secure Data Storage – Loss of personal data is a serious matter, and if this occurs, it must be self-declared under GDPR rules. The CCTV data storage component should be password protected and kept in a secure place, particularly bearing in mind that serious criminals might seek-out this unit to destroy evidence of their activities.

Is my CCTV system really a CLOSED Circuit system as the name implies? Many CCTV systems, even basic ones, can now be set-up so that images can be remotely accessed via smartphone, and with real-time alerts being sent to the phone. Consideration should to be given as to whether this remote access function is necessary or even desirable in the case of a church. Similarly, if data is streamed to storage in the *Cloud*, consideration should be given as to its security.

Subject Access requests – Individuals can request sight of their personal data. Consideration needs to be given as to how to comply with such requests without breaching others’ privacy rights. There may also be requests for footage that isn’t covered by subject access requests, for example the Police investigating the theft of a handbag in church. However, there are also potential problems with third party requests – a practical example might be a parishioner requesting footage of their car being pranged by another driver in the church carpark for the purpose of an insurance claim.

What signage should we use? Signage should be compliant with legislation and should ideally include the legal basis for processing the data (for example ‘the safety of visitors, the protection of property, and crime prevention’), the data controller’s name (the Diocese) and contact information for complaints or queries. Off-the-shelf plastic signs are available from sign retailers, which can be personalised as needed. Note that signage should be large enough to be easily noticed by visitors and should be positioned so that they see it as soon as they enter a monitored area – for example, a car park entrance should have large clear signage if CCTV covers this area. A second sign could be placed somewhere close to the church entrance so that it is clear that this area is covered too (the legal basis for monitoring and recording images inside and outside may also be different). Strictly speaking, there is a difference between ‘monitoring’ and ‘recording’, though most signs do not differentiate between these.



*Note that a Code of Practice for CCTV users and a Self-Assessment Tool is available via the Surveillance Camera Commissioner’s website.*

**Appendix 2**

**Guiding Principles**

Extract from the Surveillance Camera Code of Practice

System operators should adopt the following 12 guiding principles:

1. Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.
2. The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.
3. There must be as much transparency in the use of a surveillance camera system as Possible, including a published contact point for access to information and complaints.
4. There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.
5. Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.
6. No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.
7. Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.
8. Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.
9. Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.
10. There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.
11. When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

**Appendix 3 (please use this as a template but add your parish name/logo etc.)**

**CCTV Camera Location Log**

Please list all cameras in and around the parish, owned and operated by the parish:

|  |  |  |
| --- | --- | --- |
| **Camera Number/****Reference** | **Camera Location** | **Camera type***e.g. fixed, motion activated,* *wireless etc.* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

(Please continue on separate sheet if needed)

**Appendix 4 (please use this as a template but add your parish name/logo etc.)**

**CCTV Functionality Log**

Please use this form to check that your CCTV system is working correctly. It is suggested that this is done weekly.

Please print further copies of this template for your use.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Date of review:**  | **Date/time correctly displayed?** | **Are images in focus?** | **Are cameras****functioning properly?** | **Comments:***List any fault and/or functionality exceptions, stating location of the camera(s) and date fault was rectified.* | **Reviewer’s name & signature:** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Appendix 5 (please use this as a template but add your parish name/logo etc.)**

**CCTV Incident Log**

***Please print and keep blank copies of this form for your use.***

Parish Name/Area: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Incident date: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . Incident time: . . . . . . . . . . . . . . . . . . . . . .

Report competed by: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Where did the incident take place?

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**What type of incident is this?**

□ Threat □ Physical injury □ Damage to property / assets

□ Theft □ Other (please specify) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**Has this been reported to the Police?** □ Yes Date reported: . . . . . . . . . . . . . . . . . □ No

If no, please give reason: . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

If yes, please provide the Crime Reference Number? . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

**Has this been reported to the Insurer?** □ Yes Date reported: . . . . . . . . . . . . . . . . . □ No

Which camera(s) captured the image(s)? . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Has the footage been kept for evidential purposes?

□ Yes □ No

Have any of the following made a request for the footage?

□ Police □ Insurer □ Member of the public

□ Other (please specify) **. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .**

**Please contact the DPO (0207 798 9015 or dpo@rcdow.org.uk) where a request for stills/footage has been made and before anything is disclosed to the enquirer.**

What has been requested?

□ Still photo □ CCTV footage

A written request for stills/footage must be received in writing and attached to this form, stating the nature of the incident as well as date and approximate time of the incident.

Has proof of enquirer been verified?

□ Yes □ No □ How was this verified? . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Has this been disclosed?

□ Yes □ No

Incident details: Please provide full details of the incident. Attach further pages if required.

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .