

INFORMATION MANAGEMENT POLICY

1. This policy sets the principles for the management of information in the Investigation. It explains how the Investigation will manage information appropriately in order to comply with relevant legislation, to meet the needs of the Investigation and to create an independent report.
2. This policy should be read alongside the Investigation's Operational Protocol which is available on the Investigation's website (www.iqci.org.uk).

Legal requirements for information management

3. The Investigation has been established under s.71 of the Government of Wales Act 2006, which empowers the Welsh Ministers, First Minister or Counsel General to "*do anything... which is calculated to facilitate, or is conducive or incidental to, the exercise of any of their other functions.*" The Welsh Government considers that the relevant function is that contained in s.48 of the 2006 Act.
4. The Investigation agrees with the Welsh Government that its records are Welsh Public Records within the meaning of s. 148 of the Government of Wales Act 2006.
5. Other relevant legislation includes the Data Protection Act 1998, the Data Protection Act 2018, the General Data Protection Regulation ('GDPR'), the Public Records Act 1958 and the Human Rights Act 1998. These assign a legal responsibility to value, protect and store information so that it is of use to the business and to create an archive at the end of the Investigation. By

following this policy the Investigation will be able to deliver on this responsibility.

6. The Investigation is also bound by the terms of its Operational Protocol.

Principles

7. In order to meet our statutory requirements, the Investigation undertakes:
 - Only to collect, process and retain information that is necessary for the conduct of the Investigation;
 - To ensure that the information that we hold is as accurate as possible;
 - To keep information no longer than is necessary;
 - To maintain an accurate record of data we process;
 - To ensure that information is processed in a way that ensures the security of any personal data;
 - To create a permanent record pursuant to the Investigation's duties under the Public Records Act.

Roles and responsibilities

8. The Investigator has ultimate responsibility for the Investigation's records and must ensure that appropriate functions, policies and procedures are in place to support the Investigation during its lifetime and to produce a permanent record once the final report has been published.
9. All members of the Investigation team will ensure that comprehensive records are kept of the Investigation's activities, are required to work in the corporate information systems so that records are available to others, and that records are managed in line with our retention and disposal policy.
10. The Secretary of the Investigation is responsible for maintaining a record of the data processed by the Investigation and is responsible for managing the risks of poor information management.

11. The Data Protection Officer assists the Investigation in monitoring internal compliance with data protection laws, informs and advises on the Investigation's data protection obligations and acts as a contact point for data subjects. The Data Protection Officer acts as Senior Information Risk Owner (SIRO) and is responsible for managing the risks of poor information management.

Scope of this policy; business information and evidential material

12. Business information includes any document which is generated by the Investigation during the course of its work. It does not include evidential material supplied by providers of information.
13. The records of the Investigation will be held digitally. Hard copy documents received or generated by the Investigation will be copied and held digitally and either returned to their source or destroyed. Significant emails will be retained.
14. Business information will be retained so that important records survive which capture:
 - key decisions and how those decisions were reached (e.g. minutes of meetings, correspondence prior to and after the meeting that result in a decision being made and/or an action taken forward)
 - how procedures work (e.g. standard operating procedures and changes to them), and
 - contractual/purchasing arrangements (e.g. service delivery contracts, purchase orders).
15. Evidential documents and statements are expected from contributing organisations and individuals. These will be managed so that information is available only to those who need to access and share it in order to ensure that work is carried out securely and effectively.

Lawful basis for data processing under the GDPR

16. The Investigation's lawful basis for processing personal data is that it is necessary for it to perform a task in the public interest, namely the carrying out of the Investigation within its terms of reference.

17. The Investigation's lawful basis for processing 'special category data' is that the processing is necessary for reasons of substantial public interest, on the basis of 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.

Business Processes

18. The following is a summary of the processes that the Investigation will follow:
 - The Investigation has issued a Call for Evidence to invite the submission of evidence (for example information, documents and witness statements);
 - All evidence received will be securely stored within the Investigation's Digital Document Management System ('DDMS');
 - Evidence will be reviewed and categorised to identify sensitive confidential information that may need to be redacted;
 - During the investigation, some evidence may be shared with Core Participants to the Investigation (see the Core Participant policy on the Investigation's website);
 - Private hearings will take place where some evidence and information will be referred to by the Investigation team and witnesses;
 - A report will be written, drawing on the evidence received;
 - After the Investigation concludes, a record of the Investigation including

key evidence will be preserved and stored securely. Neither current or future Welsh Ministers nor their Special Advisors will have access to the Investigation's record.

Confidentiality and sharing and handling of data

19. The Investigator may use any information (including documents) provided to it for the purpose of fulfilling its Terms of Reference:
 - a. It will sometimes be necessary for the Investigation to share information with people such as the Core Participants. This will be done securely in line with Government security protective marking and data handling procedures, as well as in compliance with the Operational Protocol (particularly paragraphs 16, 17, 20, 21 and 22).
 - b. Subject to paragraph 14 above and the Operational Protocol, personal data will not be shared with others unless it is required by the Terms of Reference and the Investigation considers it necessary to share such data.
 - c. Information will be published in the Investigation's final report, where it is necessary to do so, in compliance with the Operational Protocol (paragraph 21) and within the Terms of Reference.
 - d. If the Investigator considers it necessary to publish information in order to comply with its duty under Article 10 ECHR or its common law duties, he will do so in compliance with paragraph 22 of the Operational Protocol.

20. Any information which is provided to the Investigation under express conditions of confidentiality will not be disclosed to others or published without the individual's consent.

21. In line with paragraphs 16-17 of the Operational Protocol, the Investigation will not do anything which provides a means of identifying a complainant in relation

to the conduct of Carl Sargeant unless they have given their prior consent to the disclosure.

22. The Investigation is registered with the Information Commissioner's Office as a data controller because the Investigation decides how both personal and sensitive personal data (or special category data under the GDPR) are processed. Given the nature of the subject matter that the Investigation covers, the team will be advised how to take appropriate care when handling personal data to ensure that breaches of the Data Protection Act 2018, the GDPR and Investigation policies do not occur.

Requests under the Freedom of Information Act

23. The Investigation is an "inquiry" for the purposes of the Freedom of Information Act 2000. Therefore, while the Investigation is in the course of its work and before its conclusion, the Act does not apply and any requests for information made under the Act will not be considered.

Security of information

24. The Investigation team will adhere to document handling and clear desk policies. Staff will observe the need for security when working from home by not removing physical material from the office environment or hearings. As far as possible, digital documents will not be printed; where it is necessary to print, paper copies will be securely destroyed as soon as they are no longer needed. Staff will not use personal email accounts for Investigation business.

Retention and disposal of information

25. The Investigation will manage its records effectively and to retain them only as long as necessary to meet business needs and statutory requirements. To comply with this requirement, retention periods will be allocated to records to ensure that records for each function are retained for the appropriate length of

time, but no longer. All retention schedules will be signed off by the Investigator.

26. After the Investigation concludes, a record of the Investigation including key evidence will be placed in a secure archive in order to comply with the Investigation's duties under the Public Records Act 1958. Neither current or future Welsh Ministers nor their Special Advisors will have access to the Investigation's record.

You - How to gain access to your data

27. If we hold data about you, you are entitled to ask for a copy of it as a Subject Access Request (SAR). If you wish to know what data is held on you, or to make a Subject Access Request please contact secretary@iqci.org.uk. We do not charge for providing you with this data. You may also request that we amend or delete your data.
28. If you are dissatisfied with how the Investigation is handling your data, please contact our Data Protection Officer, Gillian Body, at dpo@iqci.org.uk