INFORMATION SECURITY INCIDENT AND INCIDENT INVESTIGATION POLICY

Version No. 9 : February 2026

First Issued: **April 2017**
Review date: **February 2029**

Contents

*(For quick access to a specific heading - **press CTRL and click your mouse** to follow the link for the below options)*

1. INTRODUCTION

ECCH, herein after referred to as “The CIC”, is highly reliant on information that is captured, stored, processed and delivered by computers and their associated communication facilities.

Such information plays a vital role in supporting business processes and customer services, in contributing to operational and strategic business decisions and in conforming to legal and statutory requirements.

Accordingly, the information and the enabling technologies are important assets that will be protected to the level commensurate with their value to the organisation. Special care will be taken to ensure that Person Identifiable and business/corporate confidential information is not compromised.

2. PURPOSE

The purpose of this policy document is to ensure that staff are aware of their individual responsibilities in relation to Security Incidents and the Investigation of the CIC’s systems.

3. SCOPE

This Policy applies to all ECCH staff (including substantive/temporary employees and any contractor, agency, student, honorary and volunteer workers) who may be involved in or asked to be involved in a security incident or the investigation of a security incident.

Any breach of or refusal to comply with this policy is a disciplinary offence which may lead to disciplinary action in accordance with the organisations Disciplinary Policy, up to and including, in appropriate circumstances, dismissal without notice.

4. DEFINITIONS

The following definitions are intended to provide a brief explanation of the various terms used within this policy.

Term	Definition
Policy	A policy is a formal written statement detailing an enforceable set of principles or rules. Policies set the boundaries within which we operate. They also reflect the philosophy of our organisation.
Data Protection Act (DPA)	The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the

	government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation 2016/679.
General Data Protection Regulation (GDPR)	The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area.
Information Governance (IG)	Information governance is a holistic approach to managing corporate information by implementing processes, roles, controls and metrics that treat information as a valuable business asset.
Caldicott Principles	Eight principles to ensure people's information is kept confidential and used appropriately.
Computer Virus	In more technical terms, a computer virus is a type of malicious code or program written to alter the way a computer operates and is designed to spread from one computer to another.
Forensic Investigation	Forensic investigation is the act of utilising science to establish facts or evidence which is to be used for crime based trials or proceeding.

5. RESPONSIBILITIES

- **ECCH Employees** – Are responsible for the implementation of this policy and following the requirements of the policy. It is the responsibility of each employee, including temporary and contract staff, to adhere to the security policy. Any breach of or refusal to comply with this policy is a disciplinary offence which may lead to disciplinary action.

- **Chief Executive of ECCH** – Overall responsibility for the enforcement of this policy lies with the Chief Executive of ECCH

- **ECCH Managers** –Are responsible for implementing the policy within their business areas, and for adherence to the policy by their staff.

- **The Data Protection Officer and ICT Lead** – Are responsible for overseeing compliance with this policy

- **IG and Caldicott Group** – Are responsible for reviewing this policy.

6. POLICY STATEMENT

6.1.1 It is the policy of the CIC to ensure that:

- Information is protected against unauthorised access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Regulatory requirements and legislation are met.
- Information technology systems are used in a manner that prevents the release of information (by accident or deliberate/criminal act), ensures their safe use and avoids damage to the specific system or any other system to which it is connected. o Information that can be used to identify a person including confidential information about that person, business information and confidential business information is restricted to authorised users only
- Business continuity plans are produced, maintained and tested. o Information security training is available to all staff.
- All breaches of information security, actual or suspected, will be reported on to ECCH's incident reporting system and to and investigated by appropriately trained individuals within the CIC, and notified to the CIC's Data Protection Officer.

6.1.2. The lawful and correct treatment of personal information is very important to the successful delivery of health care services and to maintaining confidence in the organisation as a whole.

6.1.3. To this end all staff will adhere to the Principles of the Data Protection Act (as outlined below), Caldicott Recommendations (as outlined below), NHS guidelines (as outlined below), Human Rights Act 1998, all other relevant legislation, this policy document and any relevant professional codes of practice.

6.1.4. The General Data Protection Act Principles states that personal information:

a) **processed lawfully, fairly and in a transparent manner** in relation to individuals ('lawfulness, fairness and transparency');
b) **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed ('data minimisation');
d) **accurate and, where necessary, kept up to date;** every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) **kept in a form which permits identification of data subjects for no longer than is necessary** for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

f) p**rocessed in a manner that ensures appropriate security of the personal data,** including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

6.1.5. The Caldicott report outlines eight principles:

- **Principle 1** – Justify the purpose(s) for using confidential information.
- **Principle 2** – Only use it when absolutely necessary.
- **Principle 3** – Use the minimum that is required.
- **Principle 4** – Access should be on a strict need-to-know basis.
- **Principle 5** – Everyone will understand his or her responsibilities.
- **Principle 6** – Understand and comply with the law.
- **Principle 7** – The duty to share
- **Principle 8** - Inform patients and service users about how their confidential information is used

In addition it recommends that the NHS number should be substituted for patient identifiable data wherever possible and that where patient data is transferred it should be reduced to the minimum required for the purpose.

6.1.6. NHS Guidelines

- Information Security Management NHS Code of Practice (gateway Ref 7974)
- Records Management Parts 1 & 2 NHS Code of Practice (gateway
- Refs. 270422/1 270422/2)
- Confidentiality NHS Code of Practice (gateway ref 1656)

In addition care will be taken, particularly with confidential clinical and sensitive staff information, to ensure that the means of transferring it from one location to another are as secure as they can be. Secure email, internal mail and so called 'Safe Havens' will be used wherever possible.

6.1.7. All staff will comply with current legislation regarding the use and retention of 'Person Identifiable Data' and use of computer systems. These include, but are not limited to:

1. Data Protection Act
2. Computer Misuse Act 1990
3. Copyright, Design & Patents Act
4. Regulation of Investigatory Powers
5. Human Rights Act
6. Electronic Communications Act
7. Obscene Publications Act
8. Common Law Duty of Confidentiality
9. Contracts Act 1990

10. EU Directive on Waste Electrical and Electronic Equipment

6.1.8. Breaches of the Data Protection Act can lead to inspection from the Information Commissioner and penalties which include fines and the threat of a custodial sentence if an organisation or individual within an organisation knowingly allows a risk to personal data to exist and does nothing to mitigate it.

6.1.9. Breaches of the Computer Misuse Act carry a maximum penalty of 5 years' imprisonment or an unlimited fine.

7. PROCEDURE

7.1.1. Security Incident Management

A security incident can be any IT related incident logged to the IT Service Desk System where there is a breach of security policy or an incident where one of the three fundamental principles of Information Management & Information Technology (IM&IT) security are affected (detailed in 6.1.1).

It is the responsibility of ALL staff to identify security incidents these would then be reported to the IT Service Desk, who will then log the call. Staff must also log an incident in the ECCH Incident Reporting System.

This document details a five stage process to ensure the correct determination and handling of Security Incidents.

7.1.2. Stage 1 – Determining and Raising Security Incident

Any incident which impacts one the three fundamental principles of security is a security incident.

The three fundamental principles of security are:

- **Confidentiality** – any loss or suspected loss of person identifiable or corporate confidential information is a security incident.

- **Integrity** – any incident which may compromise accuracy or completeness of corporate information or corporate information systems is a security incident.

- **Availability** – Any loss of systems/data or illegal/not permitted access to systems/data is a security incident.

Any incident where members of IT staff have "probable cause" to believe that any breach of IT Security Policy has occurred is a Security Incident.

Acceptable reason(s) for "probable cause" include;

- Other staff have witnessed a breach,
- IT staff have witnessed a breach,
- Monitoring software has reported a breach.

Any situation where members of IT staff investigating an incident becomes aware that a breach of Security policy has occurred is a Security Incident.

Acceptable reasons include;

- Discovery of a virus,
- Discovery of unlicensed or unapproved software,
- Discovery of music or video above those supplied by the CIC,
- Discovery of pornography,
- Discovery of internet/email use beyond that permitted
- Discovery of attached hardware beyond that permitted by the removable storage and removable hardware acceptable use
- policies

Where an IT incident is believed to be an IT Security Incident the following activities will occur;

- The incident ticket status within the IT Service Desk Incident Management System must be changed to that of a Security Incident,
- Within the incident ticket IT staff must document the reason(s) why the IT incident is a security incident,
- Where relevant, all user work on the affected system must cease,
- Where relevant, all active IT operations on the affected system must cease,
- All operations previously carried out by any member of IT staff must be clearly documented (name of staff, time and date, operation carried out),
- Members of IT staff must not inform local staff that a change in incident status has occurred.
- The Information Governance Lead, a Senior IT Manager or The Head of IT must be informed immediately by IT Service Desk staff of the Security Incident and its status, where relevant any equipment involved must be isolated and monitored (any on site IT staff must remain on site and maintain full visibility of the equipment) pending confirmation of action by Information Security, an IT Senior Manager, or the Head of IT.
- The names of all involved must be clearly listed within the incident ticket.

7.1.3. Stage 2 – IG Receipt of Security Incident – Severity Setting and Requests for Investigation

- On receipt of a Security Incident the Information Governance Lead, an available Senior IT Manager or the Head of IT will make the decision as to the severity of the incident (See Appendix B).

- Any incident will be dealt with by way of the Serious Incident Policy and Protocol (See Appendix B for incident levels).
- The Information Governance Lead, an available Senior IT Manager or the Head of IT will determine if further investigation is required (See Security Incident Management Decision Tree Appendix A).
- This decision will be assisted by conferring with available technical experts.
- The names of all involved must be clearly listed within the incident ticket.
- All decisions taken will be recorded within the incident ticket in the incident management system.
- All Security incidents will be recorded on a Serious Incident (SI) Form as part of the Serious Untoward Incident management system.
- Where no further investigation is required; o If there are attending IT staff, they will be informed promptly, and after confirming update of the incident ticket, continue to resolve the incident using normal IT processes. o If there are no attending IT staff, the incident will be resolved using normal IT processes and the incident ticket updated and closed.

7.1.4. If further investigation is required:

- The Information Governance Lead, an available Senior IT Manager or the Head of IT will promptly determine if resumption of service has priority over investigation of incident.
- All actions/decisions taken will be logged, where resumption of service has priority, best efforts will be made to maintain any available evidence.
- Where investigation has priority, all service recovery work may be ceased.
- In all cases, an Investigating officer will be assigned and monitoring of the
- equipment/software will be enabled,
- All information recovered will be stored on a write once media (CDR / DVDR).
- The details of CD/DVD contents, the date it was collected and names of both the Investigating Officer and the member of IT staff collecting the data must be recorded on the disk,
- Any on site IT staff will be informed that investigation is ongoing, they will not tell other on site staff,
- The manager who has made the decision as to further investigation will (at their discretion) inform other
- Involved managers/staff as to the ongoing investigation and inform on site staff of any further actions required.
- Any investigation will be reviewed on a regular basis within a timescale that at the discretion of the Information Governance Lead and based on a case by case judgement.
- At any point during the investigation the Information Governance Lead may request a forensic investigation or may terminate the investigation with due cause. (See Security Incident Management Decision Tree - Appendix A).
-

7.1.5. If the decision is to terminate the investigation.

- All decisions taken and all reasons for decisions will be logged, if there are attending IT staff, they will be informed promptly, and after confirming update of the incident ticket, continue on to resolve the incident using normal IT processes.
- If there are no attending IT staff, the incident will be resolved using normal IT processes and the incident ticket updated and closed.

7.1.6. If the decision is to request a forensic investigation.

- Any such request will be recorded within the incident ticket in the IT Service Desk Incident Management System and will clearly state the scope of the forensic examination.
- Where forensic investigation is required the Information Governance Lead, an available Senior IT Manager or The Head of IT will assign a Principal Investigator and list their name within the incident ticket in the incident management system.
- Any forensic investigation must be overseen by two members of staff. One of whom must be the Principal Investigator.
- The Principal investigator is responsible for establishing and updating the appropriate paperwork and retaining this in a secure manner.
- If the Principal Investigator suspects a member of IT staff with access to the IT Service Desk Incident Management System all investigation documents and records will be removed from the IT Service Desk Incident Management System and stored in a separate system.
- All involved members of staff will be documented in the incident ticket in the IT Service Desk Incident Management System.
- Where forensic investigation is required any attending member of IT staff will wait for confirmation from Information Governance before securing any evidence.
- Where forensic investigation is required the Information Governance Lead will take the decision whether or not to inform applicable managers and departments of the fact that an investigation is in progress.
- Should the Information Governance Lead deem it so, the owner(s)/guardian(s) of the equipment and their line manager will be informed of the fact that an investigation is occurring and the scope of the investigation. This information will be supplied verbally by the attending Principal Investigator and at a later date in writing by the Head of IT.

7.1.7. Stage 3 – Forensic Investigation - Secure and store evidence

- All evidence must be gathered with the presumption that it will be required in court.
- All evidence must be gathered with reference to the Association of Chief Police Officers Good Practice Guide for Computer based Electronic Evidence.
- Forensic investigation will not be carried out on site.
- All equipment required for forensic investigation will be documented and secured in evidence bags. The evidence bags must be signed by the attending member of IT and a local manager responsible for

- All seized equipment will be transported carefully back to a secure area for storage.
- Any transfer of equipment from investigator to storage or from storage to investigator will be documented.
- All equipment will be stored in a secure area, with restricted and documented access.
- All equipment will be stored so that no evidence can be changed deliberately or accidentally and in such a way that no evidence can be deleted purely by period of storage.
- Any data required for investigation (audit logs, proxy logs, e- mail) will be requested from the appropriate departments. The Principal Investigator must be present when this data is recovered.
- All such data will be stored on a write once media (CDR / DVDR). The details of CD/.DVD contents, the date it was collected and names of both the Principal Investigator and the member of IT staff collecting the data will be recorded within the incident ticket in the incident management system.

7.1.8. Stage 4 – Forensic Investigation

- All investigation will be carried out in a secure area separate from any other teams or individuals.
- The Principal Investigating officer will witness and guide the investigation.
- Other than documenting the investigation the Principal Investigator should not carry out technical operations unless technically qualified and authorised by management.
- All actions carried out will be documented.
- The name(s) of the person(s) carrying out the action and the name of the Investigating (witnessing) Officer will be recorded together with the date and time of investigation.
- The investigation will be limited to the original scope detailed in the incident ticket.
- No actions will be carried out that may in any way affect the original data.
- If the investigation confirms the existence of a Security Breach; o The investigation will be immediately suspended, o The incident ticket will be amended to confirm a security breach, o All equipment will be secured in evidence bags and returned to storage.
- If the investigation reaches the limit of its scope and does not confirm the existence of a Security Breach;
    - The investigation will be suspended,
    - The incident ticket will be amended to confirm no security breach,

7.1.9. Stage 5 – Actions on completion of Forensic Investigation

7.1.9.1. Where the investigation does not confirm the existence of a Security Breach;

- The Information Governance Lead may extend the scope of the investigation, inform all applicable parties and request that the Principal Investigator investigate further.

or,

- The Information Governance Lead may terminate the investigation and inform all applicable parties.
- In either case the decision will be documented in the incident ticket. In the latter case the equipment will be returned to the IT department for return to the user.

7.1.9.2. Where the investigation confirms the existence of a non-criminal Security Breach;

- The Information Governance Lead will decide, with the assistance of other involved managers, a suitable course of action. This course of action must be detailed in the incident ticket and will include the names of all involved parties together with the date and time of decision.
- Once the course of action is complete, the Information Governance Lead will inform all applicable parties, and arrange return of equipment to the IT Department for resolution of any outstanding IT issues prior to return of the equipment to the appropriate department.

7.1.9.3. Where the investigation confirms the existence of a breach of criminal law;

- The Information Governance Lead will immediately inform the Head of IT who will inform senior management.
- At the request of the Head of IT the Investigating Officer will collate all information gathered and present it to appropriate parties together with a copy of this policy, a copy of all processes used and all equipment/data involved in the investigation. Any evidence supplied will be signed for.

The Head of IT in co-operation with other Senior Management will advise the Investigating officer as to all subsequent actions the Investigating Officer must perform.

8. MONITORING AND REVIEW

This document will be reviewed by the IG and Caldicott Group, Biannually or sooner if changes in legislation occur or new best practice evidence becomes available.

9. REFERENCES

N/A

10. ASSOCIATED POLICIES & PROCEDURES *(To include but not limited to)*

- Information Governance Policy & Framework & Handbook

- Data Protection & Personal Information Handling Policy
- Confidentiality Policy
- IT Security Policy

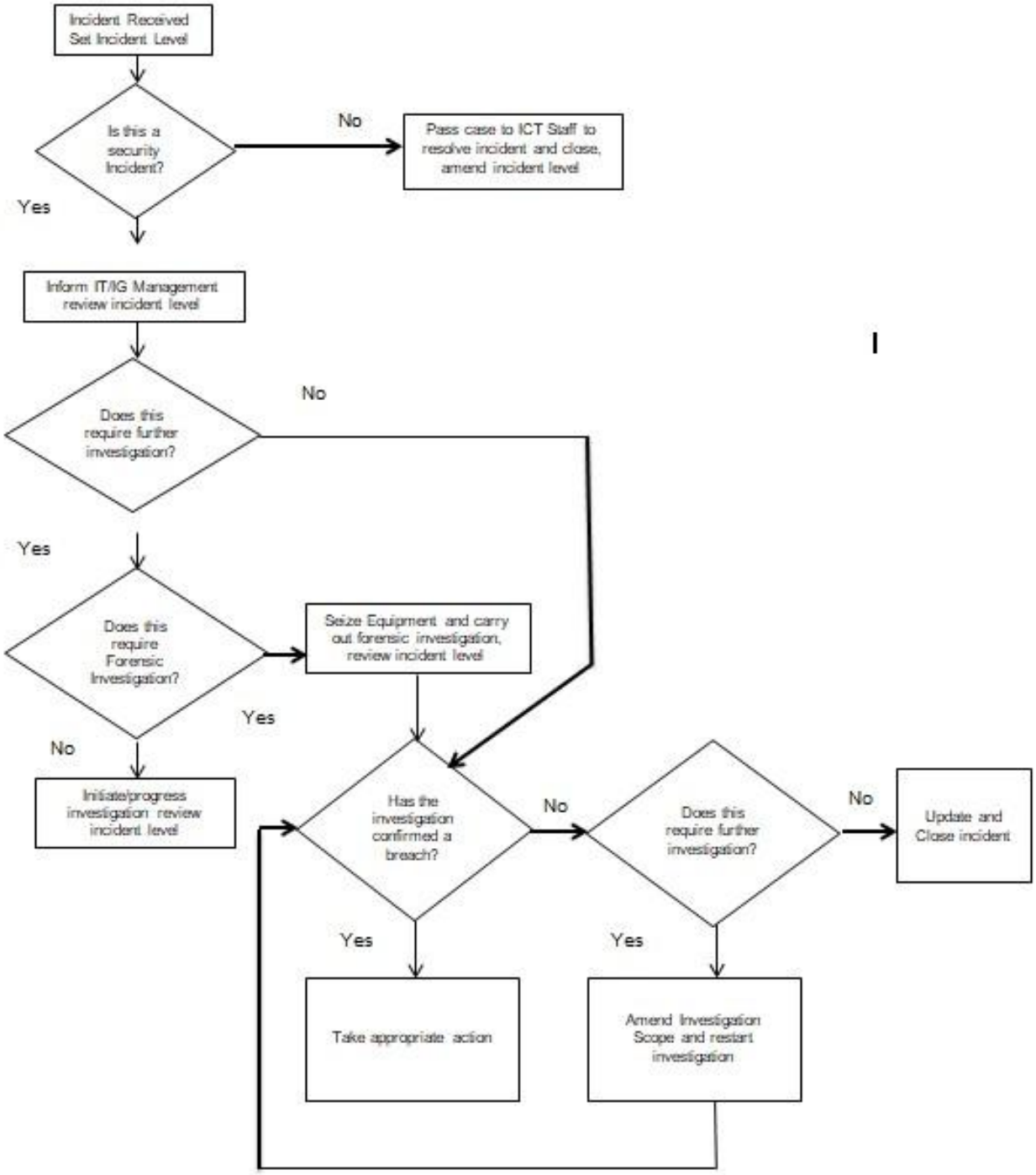
11. AUTHOR

ICT & DPO

12. APPENDICES

Appendix A - Security Incident Management Decision Tree
Appendix B – Agreed Incident Levels

Appendix A – Security Incident Management Decision Tree



Appendix B – Agreed Incident Levels

Effect on Public Perception	**0** No Significant reflection on any individual or body, Media Interest very Unlikely	**1** Damage to an individual's reputation. Possible media Interest. E.g. Celebrity Involved	**2** Damage to a team's reputation. Some local media interest that may not go public	**3** Damage to services reputation/low key local media coverage	**4** Damage to an organisation's reputation / local media coverage.	**5** Damage to NHS reputation / National Media Coverage
Data Loss	Minor breach of confidentiality only a single individual affected	Potentially Serious Breach Less than 5 people affected or risk assessed as low e.g. Files were Encrypted.	Serious Potential Breach & Risk Assessed High. E.g. unencrypted clinical records lost. Up to 20 people affected	Serious breach of confidentiality e.g. up to 100 people affected	Serious breach with either particular sensitivity e.g. sexual health details or up to 1000 people affected	Serious breach with potential for ID theft OR over 1000 people affected
Number of people affected	1	2 > 4	5 >20	21 > 100	100 > 1000	> 1000
System Loss / Loss of access to system	Single PC/Laptop/user (*Note if data is lost, see row above to set severity)	Workgroup Printer	Single Workgroup/ Single Surgery	Single Health Centre / Department Multiple workgroups / surgeries	Single CIC / Large Building / Multiple Health Centres	Entire Trust
Number of people affected	1	2 > 4	5 > 20	21 > 100	100 > 1000	> 1000

Network Failure						
Number of People affected	1	2 > 4	5 > 20	21 > 100	100 – 1000	> 1000

13. EQUALITY & DIVERSITY IMPACT ASSESSMENT

In reviewing this policy, the Policy Group considered, as a minimum, the following questions:
- Are the aims of this policy clear?
- Are responsibilities clearly identified?
- Has the policy been reviewed to ascertain any potential discrimination?
- Are there any specific groups impacted upon?
- Is this impact positive or negative?
- Could any impact constitute unlawful discrimination?
- Are communication proposals adequate?
- Does training need to be given? If so is this planned?

Adverse impact has been considered for age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion and belief, sex, sexual orientation.

Blank version of the full Equality & Diversity Impact assessment can be found here:

http://eccho/Home/FormsGuidance.aspx?udt_575_param_index=E&udt_575_param_page=2

14. DOCUMENT CONTROL

Version Date	Version No.	Author/ Reviewer	Comments
	01		
April 2017	02		
April 2018	03	Dave Shovlin	Amended by Andy Thornton
July 2020	04	Hannah Lewis	Revision of policy format and updated the General Data Protection Act Principles (page 8-9)
August 2020	05	Hannah Lewis / Chris Coleman	Minor wording changes on pages 10 & 11
April 2021	06	Hannah Lewis	Added 8th Caldicott Principle
July 2021	07	Hannah Lewis	Policy Review • Added reference to ECCH Incident and Risk Reporting System in section 6.1.1 • Added associated policies Section 8 • Added section 4 Definitions
April 2024	08	DPO	Policy Review o Updated to new template, o Updated responsibilities page as per new policy template
February 2026	09	DPO/ICT	Reviewed

DOCUMENT CONTROL SHEET

Name of Document:	Information Security Incident & Incident Investigation Policy
Version:	9
File Location / Document Name:	ECCHO
Date Of This Version:	February 2026
Produced By (Designation):	DPO & ICT
Reviewed By:	IG & Caldicott Group
Synopsis And Outcomes Of Consultation Undertaken:	
Synopsis And Outcomes Of Equality and Diversity Impact Assessment:	No adverse impact
Ratified By:-	Information Governance & Caldicott Group
Date Ratified:	09/05/2024
Distribute To:	ECCHO
Date Due For Review:	February 2029
Enquiries To:	Head of Corporate Governance (Data Protection Officer)
Approved by Appropriate Group/Committee	☐ Date: 09/05/2024