Information Security, Confidentiality and Data Protection Policy

4.5.1 Scope of the security policy

- NCEPOD's security policy aims to ensure that:
  - all systems, electronic and paper, are properly assessed for security
  - computer systems are properly maintained and monitored
  - confidentiality, integrity, and availability are maintained
  - staff are aware of their responsibilities, roles, and accountability
  - procedures to detect, report and resolve security breaches are in place
  - procedures for enabling business continuity are in place
  - procedures for regular review of the policy and procedures are in place.
- NCEPOD is committed to ensuring the security of the information it holds, in any format or on any medium.
- We regard the lawful and correct treatment of personal information as very important to our successful operation and to maintaining confidence between us and those with whom we carry out business. We will ensure that we treat personal information lawfully and correctly.
- To this end we fully endorse and adhere to the principles of the General Data Protection Regulation (GDPR).
- This policy applies to the processing of personal data in manual and electronic records kept by us in connection with our human resources function as described below. It also covers our response to any data breach and other rights under the GDPR.
- This policy applies to the personal data of job applicants, existing and former employees, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals. In addition our processes protect the patients/parents/carers whose data we hold for the necessary undertaking of our work. The Information security procedures provide greater detail on the processing of patient identifiable data.

4.5.2 Key references

- Ensuring Security and Confidentiality in NHS Organisations (E5501). NHS Executive; January 1999
- Guide to the British Standard Code of Practice for Information Security Management (PD0007). BSI; 1995
- Protecting and Using Patient Information – a manual for Caldicott Guardians. NHS Executive; March 1999
- British Standard BS ISO/IEC 17799:2000 (BS7799-1:2000) Information technology – Code of practice for information security management
- Updated ISO/IEC 27001:2013
- Data Protection Act 2018
- UK General Data Protection Regulations
- The NCEPOD Information Security Procedures, which are reviewed annually.

4.5.3 Definitions

- "Personal data" is information that relates to an identifiable person who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data.

- "Special categories of personal data" is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

- "Criminal offence data" is data which relates to an individual's criminal convictions and offences.

- "Data processing" is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- Information security can be defined as protecting the confidentiality, integrity and availability of data and information.

    - Confidentiality: protecting sensitive information from unauthorised disclosure
    - Integrity: safeguarding the accuracy and completeness of information
    - Availability: ensuring that information is available to users when required

4.5.4 Employee data held

We keep several categories of personal data on our employees in order to carry out effective and efficient processes. We keep this data in a personnel file relating to each employee and we also hold the data within our computer systems, for example, our holiday booking system.

Specifically, we hold the following types of data:

- personal details such as name, address, phone numbers
- information gathered via the recruitment process such as that entered into a CV or included in a CV cover letter, references from former employers, details on your education and employment history etc
- details relating to pay administration such as National Insurance numbers, bank account details and tax codes
- medical or health information
- information relating to your employment with us, including:
    - job title and job descriptions
    - your salary
    - your wider terms and conditions of employment
    - details of formal and informal proceedings involving you such as letters of concern, disciplinary and grievance proceedings, your annual leave records, appraisal and performance information

- internal and external training modules undertaken.

- All of the above information is required for our processing activities. More information on those processing activities are included in our privacy notice for employees, which is available from your manager.

4.5.2 Employee rights

- You have the following rights in relation to the personal data we hold on you:
  - the right to be informed about the data we hold on you and what we do with it;
  - the right of access to the data we hold on you. More information on this can be found in the section headed "Access to Data" below and in our separate policy on Subject Access Requests;
  - the right for any inaccuracies in the data we hold on you, however they come to light, to be corrected. This is also known as 'rectification';
  - the right to have data deleted in certain circumstances. This is also known as 'erasure';
  - the right to restrict the processing of the data;
  - the right to transfer the data we hold on you to another party. This is also known as 'portability';
  - the right to object to the inclusion of any information;
  - the right to regulate any automated decision-making and profiling of personal data.
- More information can be found on each of these rights in our separate policy on employee rights under GDPR.

4.5.3 Information Security and BS ISO/IEC 27001:2013 controls

- The NCEPOD Information Security Policy and procedures have been formulated in conjunction with the International Standard ISO/IEC 27001:2013 "Information technology – Code of practice for information security management". By using ISO/IEC 27001:2013 to help assess, manage, and review risks, NCEPOD demonstrates its commitment to information security and confidentiality.
- Only those controls that have been seen as being relevant to its organisational structure, business functions and goals have been selected by NCEPOD.

4.5.4 Security Management

4.5.4.1 Objective

- To establish the management structure for information security within NCEPOD.

4.5.4.2 Allocation of Information Security responsibilities

- The Chief Executive, on behalf of the Trustees, will be responsible for the overall implementation and enforcement of the Information Security Policy and will also act as the Caldicott Guardian for NCEPOD. The Deputy Chief Executive acts as the Data Controller for NCEPOD. Their responsibilities include:
  - ensuring compliance with relevant legislation
  - ensuring compliance with the Policy and procedures
  - ensuring that all staff sign confidentiality undertakings
  - ensuring that the IT Manager is aware of staff changes and access rights

- responding to breaches of information security
- reporting any breaches of security to the Trustees.

- The IT Manager is responsible for:
  - ensuring that all staff are trained in the secure use of computer systems and aware of any changes to information security procedures
  - ensuring that no unauthorised access to the computer system is permitted
  - ensuring appropriate levels of access to the computer system are maintained
  - ensuring procedures are in place to minimise the risk of theft/fraud/disruption of systems
  - maintaining an inventory of all hardware and software owned by NCEPOD
  - ensuring the appropriate administration of password protection
  - administering the NCEPOD computer network.

- All staff are responsible for:
  - operating within the parameters laid down in the NCEPOD information security procedures
  - ensuring that no breaches of information security result from their actions
  - reporting any security incidents or queries to the IT Manager.

- The Chief Executive, IT Manager, and Clinical Researchers form the NCEPOD Information Security Forum. This forum meets quarterly and is responsible for the operational management of the security system, including:
  - monitoring and reporting on the state of information security within NCEPOD
  - ensuring that the Information Security Policy is implemented throughout NCEPOD
  - developing detailed procedures to maintain security
  - ensuring that staff are aware of their responsibilities for information security
  - monitoring for actual or potential breaches of information security
  - approving major initiatives to enhance information security
  - reviewing and approving the Information Security Policy and overall responsibilities.

4.5.4.3 Review and audit

- The Policy, its implementation, and systems, will be subject to regular review by the Information Security Forum, utilising external support and advice where necessary.

4.5.5 Lawful bases of processing

- We acknowledge that processing may only be carried out where a lawful basis for that processing exists and we have assigned a lawful basis against each processing activity.
- Where no other lawful basis applies, we may seek to rely on consent in order to process data.
- However, we recognise the high standard attached to its use. We understand that consent must be freely given, specific, informed and unambiguous. Where consent is to be sought, we will do so on a specific and individual basis where appropriate. For example, employees will be given clear instructions on the desired processing activity, informed of the consequences of their consent and of their clear right to withdraw consent at any time.

4.5.6 Access to data

- Everyone has a right to access the personal data that we hold on them. To exercise this right, a Subject Access Request should be made to the Chief Executive. We will comply with the request without delay, and within one month unless, in accordance with legislation, we decide that an extension is required. Those who make a request will be kept fully informed of any decision to extend the time limit.
- No charge will be made for complying with a request unless the request is manifestly unfounded or excessive, or unless a request is made for duplicate copies to be provided to the employee making the request or to a third party acting on the employee's behalf. In these circumstances, a reasonable charge will be applied.
- Further information on making a subject access request is contained in our Subject Access Request policy.

4.5.7 Data disclosures

- NCEPOD may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:
  - any employee benefits operated by third parties;
  - disabled individuals - whether any reasonable adjustments are required to assist them at work;
  - individuals' health data - to comply with health and safety or occupational health obligations towards the employee;
  - for Statutory Sick Pay purposes;
  - HR management and administration - to consider how an individual's health affects their ability to do their job;
  - the smooth operation of any employee insurance policies or pension plans;
  - to assist law enforcement or a relevant authority to prevent or detect crime or prosecute offenders or to assess or collect any tax or duty.
- These kinds of disclosures will only be made when strictly necessary for the purpose.

4.5.8 Third party processing

- Where we engage third parties to process data on our behalf, we will ensure, via a data processing agreement with the third party, that the third party takes such measures in order to maintain NCEPOD's commitment to protecting data.

4.5.9 Requirement to notify breaches

- All data breaches will be recorded on our Data Breach Register. Where legally required, we will report a breach to the Information Commissioner within 72 hours of discovery. In addition, where legally required, we will inform the individual whose data was subject to breach.

4.5.10 Training

- New employees must read and understand the policies on data protection as part of their induction.
- All employees receive training covering basic information about confidentiality, data protection, data protection complaints and the actions to take upon identifying a potential data breach.

- The nominated data controller/auditors/protection officers for NCEPOD are trained appropriately in their roles under the GDPR.
- All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and NCEPOD of any potential lapses and breaches of NCEPOD's policies and procedures.

4.5.11 Records

- NCEPOD keeps records of its processing activities including the purpose for the processing and retention periods in its HR Data Record. These records will be kept up to date so that they reflect current processing activities.

4.5.12 Data protection complaints

- You can complain to us as well as the Information Commissioner's Office (ICO) if you consider that we have infringed data protection legislation because of the way we have handled your personal data. More information can be found in our separate policy on Data Protection Complaints.

4.5.13 Data security

- All our employees are aware that hard copy personal information should be kept in a locked filing cabinet, drawer, or safe.
- Employees are aware of their roles and responsibilities when their role involves the processing of data. All employees are instructed to store files or written information of a confidential nature in a secure manner so they are only accessed by people who have a need and a right to access them and to ensure that screen locks are implemented on all PCs, laptops etc when unattended. No files or written information of a confidential nature are to be left where they can be read by unauthorised people.
- Where data is computerised, it should be coded, encrypted or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.
- Employees must always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them.
- Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless prior authorisation has been received. Where personal data is recorded on any such device it should be protected by:
    - ensuring that data is recorded on such devices only where absolutely necessary.
    - using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted.
    - ensuring that laptops or USB drives are not left where they can be stolen.
- Failure to follow NCEPOD's rules on data security may be dealt with via NCEPOD's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

4.5.6 NCEPOD Information Security Key Points

- The following points are intended to reinforce and not replace the NCEPOD Information Security Procedures. The relevant sections of the security procedures should be still read and understood by all staff. References in brackets relate to the appropriate section in the procedure document.

4.5.6.1 Locking workstations (20.4.7)

- Machines must not be left unattended in an unlocked state. Press CTRL-ALT-DEL and the select 'Lock Computer' to lock a machine.

4.5.6.2 Password Policy (11.4)

- Passwords are changed every 60 days; the system enforces this. Passwords should never be told to another person or recorded anywhere.
- Passwords should contain both letters and numbers and be at least 8 characters in length.
- Sensitive information that is sent/taken outside of the NCEPOD network must be password protected with the recipient being informed verbally of the password used.

4.5.6.3 Virus policy (15.4)

- Unauthorised software should not be installed or executed on any computer on the NCEPOD network, including patches or upgrades, without the permission of the IT Manager.
- Any suspected or actual virus infection should be reported to the IT Manager as soon as practical.
- The installation of antivirus software on machines on the NCEPOD network should not be interfered with.

4.5.6.4 Unsolicited Email policy (17.3.6)

- All unsolicited or suspicious email should be moved to the Spam Email folder immediately.

4.5.6.5 E-mail protocols (17.3)

- NCEPOD provides electronic mail for business communications, to be used in performing assigned job duties. Staff should fully familiarise themselves with the guidelines for appropriate usage outlined in Sections 17.3.1 to 17.3.7, and Section 19.4, of the Information Security Procedures.
- Inappropriate use of email may result in disciplinary action being taken. Flagrant abuse of NCEPOD's email policy is treated as gross misconduct. NCEPOD reserves the right to monitor email usage to ensure that official NCEPOD policy is not contravened or abused.
- Emails have become an accepted method of both internal and external communications, often replacing the "written" letter and memo. The informality and ease of use of e-mail is its virtue but it is necessary to ensure that this informality is not viewed by colleagues or external contacts as unprofessional, and of a lesser standard than would be adopted for letters and memos. It is important to remember that the content of emails is regarded as a form of publication and are subject to the law of libel.

- The following protocols have been defined for use by all staff to ensure clarity and professionalism in all our communications:
  - do not assume that the recipient will be able to identify you from your name. Unless you are confident then you should state your name and title, and whether you are writing in your own name or on behalf of a colleague
  - be professional when sending e-mails. Remember that emails can be printed and retained
  - be clear whether you are providing information or requiring a response and, if so in what timescale
  - emails are not guaranteed to reach the destination that they are intended for. If the content of the email is important, and requires a response, it may be wise to follow up the email with a phone call, or to send a copy of the information sent via the regular post
  - always check the spelling and readability of informal notes
  - always use the "signature" included in the NCEPOD email template on all emails. "This email contains information intended for the addressee only. It may be confidential and may be the subject of legal and/or professional privilege. Any dissemination, distribution, copyright, or use of this communication without prior permission of the addressee is strictly prohibited. If you have received this in error, please contact the sender and delete the material from your computer".
  - do not use the email facilities to distribute any material that is illegal, pornographic, racist, sexist, homophobic or likely to cause offence in any way nor any material which may harm the organisation's reputation. NCEPOD will regard any such activity as a disciplinary offence to be dealt with through the standard disciplinary procedures.

4.5.6.6 Data Protection (18.0)

- The UK General Data Protection Regulations (GDPR) gives certain rights to individuals about whom information is held (manually or electronically). Individuals may ask for information about themselves, challenge it if appropriate or request that their data be omitted from processing. The GDPR places responsibilities on those organisations as both controllers and processors who record and use personal data.
- Under GDPR, all personal data obtained and held by us must be processed according to a set of core principles. In accordance with these principles, we will ensure that:
  - processing will be fair, lawful and transparent
  - data be collected for specific, explicit, and legitimate purposes
  - data collected will be adequate, relevant and limited to what is necessary for the purposes of processing
  - data will be kept accurate and up to date. Data which is found to be inaccurate will be rectified or erased without delay
  - data is not kept for longer than is necessary for its given purpose
  - data will be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
  - we will comply with the relevant GDPR procedures for international transferring of personal data.

- The principle of accountability also applies to data controllers who should be able to demonstrate that they comply with these principles.
- The risks to the organisation of failing to comply with the requirement of the Act are clear. Not only is there risk of criminal sanctions but also the risk of public embarrassment over failure to comply. It is also worth remembering that where an offence under the Act is committed by an organisation any employee is personally liable if the offence is attributable to neglect on their part.

4.5.6.7 Subject access (18.1)

- All subject access requests should be referred to the Chief Executive. Responses will be made within a month of request. There will be no charge for data access.

4.5.6.8 Compliance (ISO A.18) (28.0)

- NCEPOD acknowledges the importance of complying with all appropriate criminal and civil law, regulations, or contractual obligations.
- NCEPOD considers this when designing the procedures for NCEPOD's information processing facilities and in all data handling tasks seeks to comply fully with the appropriate regulations.
- The Chief Executive, on behalf of the Trustees, is responsible for ensuring compliance with all relevant legislation.
- All relevant statutory, regulatory, and contractual requirements are considered when designing and documenting information systems and processes. Any specific controls and individual responsibilities necessary to meet these requirements are similarly defined and documented.
- All new legal, regulatory, and contractual agreements will be reviewed for any necessary changes to the security policy.
- NCEPOD is registered as a Data Controller. The Chief Executive and Deputy Chief Executive, on behalf of the Trustees, have responsibility for compliance with the Data Protection Act 2018 and the UK General Data Protection Regulations.
- NCEPOD complies with the legal restrictions on the use of material in respect of which there may be intellectual property rights, such as copyright, design rights, and trademarks. NCEPOD complies with legal restriction on the use of licensed software and promotes an internal policy of legal usage.
- All legal, statutory, or regulatory requirements for maintaining records are complied with. Information is classified by type, and this classification is used to ascertain the necessary period of retention (in conjunction with the guidelines for retention of data given in Appendix E of the Information Security Procedures).
- All organisational records are securely stored to prevent loss or destruction to important and sensitive information.
- Where any action to be taken involves the law, either civil or criminal, NCEPOD will conform to the rules of evidence as laid down in the relevant law, or in the rules for the specific course in which the case will be heard. NCEPOD will take relevant advice on each individual matter, covering the admissibility, quality and completeness, and consistency of the evidence.
- The information processing facilities provided by NCEPOD are for business use. NCEPOD reserves the right to monitor use of the facilities to detect and prevent improper usage.

Where any targeted monitoring takes place, the staff member(s) involved will be informed prior to the monitoring occurring.

- Where appropriate, a message will be prominently displayed at the log on stage indicating that the system being entered is private and that unauthorised access is not permitted.

4.5.6.9 Personnel security (29.0)

- To reduce the risks of human error, theft, fraud, or misuse of facilities, NCEPOD addresses security considerations at the recruitment stage, and within staff contracts.
- Verification checks are made at the time of job application for permanent staff positions (Section 29.2 of the Information Security Procedures).
- Screening and due diligence should be carried out for contractors and temporary staff, where they will be handling sensitive information.
- Where temporary staff are provided through an agency, the contract with the agency should clearly specify the agency's responsibility for screening and the notification procedure they need to follow if screening has not been completed or if the results give cause for doubt or concern.
- Management should evaluate the supervision required for new and inexperienced staff with authorisation for access to sensitive systems.
- All staff are bound to confidentiality, and to the terms of the NCEPOD Information Security Policy, by the Terms and Conditions of their employment. The Terms and Conditions, in conjunction with the Staff Handbook, spell out the employee's rights and responsibilities.