NHS
North Tyneside
Clinical Commissioning Group

Information Governance

Staff Handbook and Code of Conduct

March 2019 to March 2022

Approved: 26/03/19
Head of Governance
V6

1. INTRODUCTION

This handbook has been produced to provide staff with the necessary information to comply with information governance legislation and national and local guidance.

All staff, whether permanent, temporary or contracted are responsible for ensuring that they comply with information governance requirements on a daily basis.

Managers and Information Asset Owners (IAOs) and Administrators (IAAs) are responsible for promoting good Information Governance and ensuring compliance by team members / colleagues.

Please remember that Information Governance is **everyone's** responsibility. You must protect any and all personal data you come into contact with during your employment with the CCG.

2. WHAT IS INFORMATION GOVERNANCE?

Information Governance is a framework for handling information in a professional, confidential and secure manner. Information assets or 'data' can be personal and relate to service users / employees, or they can be corporate (e.g. financial information).

The approach to Information Governance encompasses legal obligations, national and local guidance and best practice. The aim of Information Governance is to demonstrate that North Tyneside CCG can be trusted to maintain the confidentiality and security of personal and corporate information by helping staff to practice good Information Governance. This is supported by the North Tyneside CCG Information Governance Strategy.

Information Governance is largely concerned with data protection and is governed by the Data Protection Principles outlined under Article 5 of the General Data Protection Regulations (GDPR). These principles are:

1. Article 5.1 a) The processing of data must be lawful, fair, and transparent.
2. Article 5.1 b) The purposes of processing data must be specific, legitimate, and explicit.
3. Article 5.1 c) Processing of data must be adequate, relevant, and limited (only process when absolutely necessary)
4. Article 5.1 d) Data processed must be accurate (including the provision of rectification if found to be inaccurate).

5. Article 5.1 e) Data should be 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.
6. Article 5.1 f) Data should be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

KNOW YOUR RESPONSIBILITIES:

All staff have a duty of confidentiality regarding personal information. This is based on Data Protection and other laws. Breaches of confidence and inappropriate use of records or computer systems are serious matters which could result in disciplinary proceedings, dismissal and possibly legal action and significant fines for both yourself and the CCG.

Article 83(5) (a) of GDPR states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

3. INFORMATION GOVERNANCE POLICIES

All North Tyneside CCG Information Governance Policies are listed below. All of the policies can be obtained via the North Tyneside CCG website: https://www.northtynesideccg.nhs.uk/news-media/publications/policies/?showall

Hard copies can be obtained from Irene Walker, Head of Governance (North Tyneside CCG).

North Tyneside CCG's Information Governance Policies are as follows:

- Confidentiality and Data Protection Policy
- Data Quality Policy
- Information Access Policy
- Information Governance and Information Risk Policy
- Information Security Policy
- Records Management Policy and Strategy
- Email and Internet Acceptable Use Policy
- Social Media Policy
- Incident Reporting and Management Policy

KNOW YOUR RESPONSIBILITIES:

Please ensure that you read the above policies to make sure that you are aware of and understand your Information Governance responsibilities.

4. DATA SECURITY & PROTECTION (DSP) TOOLKIT

The DSP Toolkit is an online performance framework hosted by NHS Digital. All Health and Social Care service providers, commissioners and suppliers are required to carry out self-assessments of their compliance against a set of data security standards, of which there are ten:

- Personal Confidential Data
- Staff Responsibilities
- Training
- Managing Data Access
- Process Reviews
- Responding to Incidents
- Continuity Planning
- Unsupported Systems
- IT Protection
- Accountable Suppliers

Each standard is underpinned by several mandatory assertions against which the CCG must provide evidence to be considered compliant.

KNOW YOUR RESPONSIBILITIES:

- The DSP is a self-assessment piece of software mandated for use by NHS, social care, GPs, commercial third parties and other providers of NHS/healthcare-related services to self-audit their IG compliance.
- CCGs have 70 mandatory Assertions to complete.
- Creates a year-long IG compliance work programme each financial year, facilitated by the NECS IG Team.
- Is subject to both internal and external audit.
- Has reports available online showing whether each organisation is compliant.
- Supports the CCG in bidding for services or partnerships by demonstrating good IG practice within the organisation.

5. INFORMATION GOVERNANCE TRAINING

As of 1 October 2017 all staff should complete their Information Governance training, known as Data Security Awareness Level 1, via the e-learning for health (eLfH) site which can be accessed via this link: https://portal.e-lfh.org.uk/

To access the Data Security Awareness training you should follow the instructions below:

Select: login using user name and password contained in the email from e-LfH
Select: My e-learning
Select: Data Security Awareness (NHSD)
Select: NHS Data Security Awareness Level 1
Complete: All modules within this course

The required pass mark for the mandatory training is 80%
If you have any queries regarding your training, please contact the IG Team via necsu.ig@nhs.net

KNOW YOUR RESPONSIBILITIES:

This training is mandatory for all staff and is also a mandatory requirement of the DSP Toolkit mentioned above. The training is available 24/7 and therefore learning can fit around your existing commitments. You do not need to complete the course or a module in a single session; your progress will be saved and when you return to your learning you can pick up where you left off. The only stipulation is that the training must be completed between 1st April and 31st March **every** year.

6. CALDICOTT GUARDIAN

A Caldicott Guardian is a senior figure responsible for protecting the confidentiality of service user / employee information and enabling appropriate information sharing. The Caldicott Guardian has a strategic and advisory role which involves representing and championing Information Governance requirements and issues at Board or management team level and at other levels where appropriate. The Caldicott Guardian is a member of the Governing Body and works closely with the Senior Information Risk Owner (SIRO) and Governance Lead who are represented on that group.

KNOW YOUR RESPONSIBILITIES:

Dr Ruth Evans is the Caldicott Guardian for North Tyneside CCG.

Before you handle or disclose any confidential information you should use the Caldicott principles as a guide. The seven Caldicott principles are as follows:

1. **Justify the purpose(s) for use of confidential information**
   Every proposed use or transfer of personal confidential data within or from an organisation should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed, by an appropriate guardian.

2. **Don't use personal confidential data unless it is absolutely necessary**
   Personal confidential data should not be included unless it is essential for the specified purpose(s) of that flow. The need for patients to be identified should be considered at each stage of satisfying the purpose(s).

3. **Use the minimum necessary personal confidential data**
   Where use of personal confidential data is considered to be essential, the inclusion of each individual item of data should be considered and justified so that the minimum amount of personal confidential data transferred or accessible as is necessary for a given function to be carried out.

4. **Access to personal confidential data should be on a strict need-to-know basis**
   Only those individuals who need access to personal confidential data should have access to it, and they should only have access to the data items that they need to see. This may mean introducing access controls or splitting data flows where one data flow is used for several purposes.

5. **Everyone with access to personal confidential data should be aware of their responsibilities**
   Action should be taken to ensure that those handling personal confidential data – both clinical and non-clinical staff – are made fully aware of their responsibilities and obligations to respect patient confidentiality.

6. **Comply with the law**
   Every use of personal confidential data must be lawful. Someone in each organisation handling personal confidential data should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers.

   If you are still unsure on review of the Caldicott principles please contact your line manager or the NECS Information Governance Team on 0191 375 1769.

   Ultimately, the Caldicott Guardian will make the final decision as to what, when and how personal identifiable information is used, received or sent within North Tyneside CCG.

7. NATIONAL DATA GUARDIAN REVIEW

The National Data Guardian completed a review of data security in 2016 out of which came the following recommendations:

Leadership Obligation 1: People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1: All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2: All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2: Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4: Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6: Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7: A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3: Technology: Ensure technology is secure and up-to-date.

Data Security Standard 8: No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9: A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10: IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

KNOW YOUR RESPONSIBILITIES:

Everyone who works within the NHS and with personal data should be aware of the Caldicott Principles, the Data Protection Principles, and the Data Security Standards. Compliance with the spirit of these key principles and standards is therefore a fundamental building block for good data protection practice. It is also key to your compliance with the detailed provisions of data protection legislation.

8. CONFIDENTIALITY

Common law is not written out in one document like an Act of Parliament. It is a form of law based on previous court cases decided by judges and is also referred to as 'case law'. The law is applied by reference to previous cases and is said to be 'based on precedent'.

The general position is that, if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent or some other legal basis. In practice this means that all personal information, whether held on paper, computer, visually, audio recording or held in the memory of a professional, must not normally be disclosed without a legal basis for doing so.

All employees are responsible for maintaining the confidentiality of information gained during their employment, this also extends after they have left the employment of North Tyneside CCG. This is not only a contractual requirement but also a requirement of the Data Protection Act 2018. Employees should also protect the confidentiality of information that is classed as commercial in confidence; this information should be treated with the same care as personal confidential information.

KNOW YOUR RESPONSIBILITIES:

No employee shall breach their legal duty of confidentiality, allow others to do so, or breach any of the organisation's security systems or controls.

The Health and Social Care (Safety and Quality) Act 2015 introduced a legal duty requiring health and adult social care bodies to share information where this

will facilitate care for an individual. This information is in the form of a single identifier, the NHS number. Health and adult social care commissioners and providers, including those contracted to provide services, need to consider the circumstances where information can be lawfully shared and the information that might facilitate the provision of health services and adult social care. There are several different types of information:

1. **Personal (non-sensitive)** – Personal data is information recorded about an individual that enables them to be identified. In order to lawfully process personal data, you must identify a lawful basis under GDPR Article 6. Personal data can include one or more of the following examples:

- ✓ Name
- ✓ Date of birth
- ✓ Address
- ✓ Postcode
- ✓ Next of kin
- ✓ Carer's details
- ✓ National insurance number
- ✓ Bank details
- ✓ Unique identifier e.g. NHS number

2. **Personal (sensitive)** – Sensitive personal data (also known as 'special category data) is personal data which the GDPR says is more sensitive, and so needs more protection. In order to lawfully process special category data, you must identify both a lawful basis under GDPR Article 6 and a separate condition for processing special category data under GDPR Article 9. These do not have to be linked. Some examples of personal sensitive data are:

- ✓ Medical conditions
- ✓ Sexual orientation
- ✓ Religious beliefs
- ✓ Political views
- ✓ Ethnic origin
- ✓ Criminal convictions
- ✓ Trade union membership
- ✓ Genetic and biometric data

3. **Corporate** – Corporate information belongs to an organisation or company and can be considered 'sensitive' at a commercial level, for example:

- ✓ Contract information
- ✓ Minutes of meetings
- ✓ Finance details

4. **Anonymised data** – Is personal or personal sensitive data than has been altered so that individuals can no longer be identified and it is virtually impossible to re-identify them. Anonymised data can be shared lawfully and where this might facilitate care it must be shared.

5. **Pseudonymised data** – Pseudonymisation takes the identifying fields within a data set and replaces them with artificial identifiers, or pseudonyms (such as a code or reference number). The purpose is to render the data record

less identifying and therefore reduces concerns with data sharing and data retention. The difference between this and anonymised data is that individuals can still be identified by pseudonymised data if access to the re-identifying codes is provided.

Where information is associated with an identifiable individual (personal information or personal sensitive information) then the individual concerned should be informed about how and why it is processed and with whom it may be shared for it to be lawful. The CCG informs individuals about how it processes data via it's Fair Processing Notice, which can be found here: **https://www.northtynesideccg.nhs.uk/fair-processing-notice/**

KNOW YOUR RESPONSIBILITIES:

Knowingly misusing or failing to properly safeguard any confidential data will be regarded as a disciplinary offence and (in some cases) can be a crime.

More information about information sharing can be found in Section 14. **Information Sharing**

9. CONFIDENTIALITY AUDITS

In order to provide assurance that access to confidential information is gained only by those individuals who have a legitimate right of access, it is necessary to ensure appropriate monitoring is undertaken on a regular basis.

Monitoring should be carried out to ensure that irregularities regarding access to confidential information can be identified, reported to the Caldicott Guardian and action taken to address the situation, either through disciplinary action, the implementation of additional controls or other remedial action as necessary.

Actual or potential breaches of confidentiality should be reported via SIRMS and to the NECS IG Team immediately, in order that action can be taken to prevent further breaches taking place. More serious breaches (where personal data has been breached outside of the NHS Family) must also be reported to the ICO via the DSP Toolkit within 72 hours of becoming aware of the incident. The individuals affected must also be made aware. More information on this can be found on the ICO website. https://ico.org.uk/for-organisations/report-a-breach/ and from the CCG's Incident Reporting and Management Policy.

The NECS Information Governance Team will ensure that quarterly audits of security and access arrangements are conducted on a regular basis. Areas to be audited will include:

- Security applied to manual files e.g. storage in locked cabinets/locked rooms

- Arrangements for recording access to manual files, e.g. access requests by solicitors, police, data subjects etc.
- Evidence that checks have been carried out to ensure that the person requesting access has a legitimate right to do so
- The existence and location of noticeboards containing personal information
- The use of and disposal arrangements for post-it notes, notebooks and other temporary recording material
- Retention and disposal arrangements
- The location of fax machines and answer phones which receive confidential information (if used. The use of fax machines is not recommended due to the IG risks involved)
- Confidential information sent or received via email – e.g. security applied and e-mail system used
- Information removed from the workplace – e.g. authorisation gained either for long term or short term removal
- Security arrangements applied – e.g. transportation in secure containers
- The understanding of staff within the department of their responsibilities with regard to confidentiality and restrictions on access to confidential information
- Security applied to laptops, compliance with the NECS Remote Access Policies
- Evidence of shared passwords being used within the area audited
- General physical security of premises where information is concerned.

Audits will be carried out by a series of staff IG awareness interviews / questionnaires and observations / visits.

For further information please refer to the North Tyneside CCG Confidentiality and Data Protection Policy and Confidentiality Audit Procedure

10. SENIOR INFORMATION RISK OWNER

The Senior Information Risk Owner (SIRO) is accountable for the organisation and acts as a champion in managing information assets, the risks associated with them and any incidents surrounding them.

The SIRO will also ensure that the Executive Committee is kept up to date on all information risk issues. The role will be supported by the NECS Senior Governance Manager and the organisation's Caldicott Guardian, although ownership of the Information Risk programme will remain with the SIRO.

KNOW YOUR RESPONSIBILITIES:

Lesley Young-Murphy, is the SIRO for North Tyneside CCG.

11. INFORMATION ASSET OWNERS

The SIRO is supported by an IAO (there may be more than one IAO depending on the number of information assets held by the CCG. The role of IAO is to understand what information is held and why, what is added and what is removed, who has access (and why) in their own specific area. They are therefore able to understand and address risks to the information assets they 'own' and to provide assurance to the SIRO on the security and use of the assets. The NECS Information Governance Team will support the IAO / IAOs in fulfilling their role, which includes keeping a CCG Information Asset Register up to date.

KNOW YOUR RESPONSIBILITIES:

Information is an incredibly valuable asset that must be safeguarded. It is both a Legal and DSP Toolkit requirement to maintain a list of all information assets held by the CCG and the legal basis for doing so. This demonstrates that the CCG knows what information is being processed within its premises, systems, and partners. The CCG's list of information assets is called the Information Asset Register.

12. INFORMATION ASSET ADMINISTRATORS

Information Asset Administrators (IAAs) are also required to support the CCG's SIRO and will work with the NECS Information Governance Team to ensure staff apply the Data Protection Act and Caldicott Principles within working practices.

The Information Asset Owners (IAOs) and Administrators (IAAs) within North Tyneside CCG are as follows:

Asset Area	Information Asset Owner (IAO)	Information Asset Administrator (IAA)
CCG Business Continuity Plan	Irene Walker	Susan Askew
CCG Constitution	Irene Walker	Susan Askew
CCG Gov Body (Private) and Committee papers	Irene Walker	Susan Askew
CCG Gov Body (Public) and Committee papers	Irene Walker	Susan Askew
CCG Policies and Procedures	Irene Walker	Susan Askew
CHC Database	Phil Crozier	Phil Crozier

Asset Area	Information Asset Owner (IAO)	Information Asset Administrator (IAA)
CHC Restitution files	Phil Crozier	Phil Crozier
Commissioning intentions and other planning information	Steve Rundle	Donna Sample
Complaints Information (As Controller)	Lesley Young-Murphy	Susan Askew
Contracts	Anya Paradis	Dianne Effard
CQI Toolkit	Marc Rice	Wally Charlton
Finance Spreadsheets	Jeff Goldthorpe	Sarah Turner
North Tyneside CCG Intranet (GPTeamNet) - As processor	Lesley Young-Murphy	Marc Rice
NTCCG Website	Wally Charlton	Anne Timmins
Safeguarding records	Jan Hemingway	Anne Foreman Adrian Dracup
HR Records	Lesley Young-Murphy	Anne Timmins
CCG Declaration of Interest	Irene Walker	Susan Askew
Individual Funding Request (as Controller)	Steve Rundle/Ruth Evans	Commissioning Team Admin
S117	Janet Arris	Commissioning Team Admin
SEND	Janet Arris	Commissioning Team Admin
LeDeR	Maureen Grieveson	Jan Hemingway Anne Foreman Adrian Dracup Ruth Marshall Judith Gibson
Children's Continuing Care aged 0-18 (as controller)	Janet Arris	Commissioning Team Admin

13. INFORMATION SECURITY

Smartcards

- Treat your smart card as you would your bank card and keep it in a safe place.
- Never share your smartcard with anyone.
- Do not write down your password.
- Never leave your smartcard unattended or in the smartcard reader when not in use.
- Report the theft, loss or damage to your smartcard via the SIRMS system immediately to ensure that your card is cancelled / replaced as soon as possible.
- Read, understand and sign the declaration on your RA01 form to agree your responsibilities.
- Access to personal identifiable information through clinical systems should be for a legitimate reason, any other access will be viewed as a breach of confidentiality.

Passwords

- Passwords are not to be shared or used even under supervision in training situations.
- Ensure that strong passwords are used, i.e. using a minimum 8 digit combination of letters, numbers and special characters (!?£&%$ etc.).
- Do not use consecutive passwords i.e. mypassword1, my password2, my password 3 etc.
- Do not write passwords down where they can be easily found i.e. on a sticky note next to your workstation or on your laptop.
- Change passwords when prompted.
- Change passwords immediately if you suspect that they have been compromised and report the incident via SIRMS.
- Do not base your password on something that can be easily guessed such as your own name, make of car, car registration number, pet's name etc.
- Do not recycle old passwords.

Your Work Environment

- Ensure that filing cabinets containing confidential information are locked when not in use.
- Ensure that filing cabinets are not in areas accessible to members of the public / visitors.
- Always wear your identity badge.
- Whenever possible always escort on-site visitors.
- Do not take confidential information out of the office unless on approved business.
- Safeguard the security and confidentiality of information at all times, for example lock your workstation when away from your desk.

- If confidential information is taken off site by agreement do not leave them in your car in plain sight overnight; ensure that they are stored securely.
- If they must be left in a vehicle, ensure they are out of sight and the vehicle is locked.

Printing and Photocopying

- Photocopying machines should not be situated in areas to which visitors / members of the public have access.
- No documents should be left on or in the photocopier after copying.
- Photocopying should be taken away immediately after printing.
- When printing from a PC use the locked print option.

Confidential Waste

- Ensure that you dispose of confidential information appropriately in the confidential waste bins provided.
- Confidential waste bins should be kept locked at all times.
- The organisation's approved contractor is Shred-It, the contract is managed by NHS Property Services.

Eavesdropping

- Ensure that where conversations are conducted relating to organisational business either over the telephone, face to face or in the close proximity of public/reception areas, care must be taken that personal information is not overheard by persons who do not have a legitimate need to hear such information.
- This also applies where recorded messages are re-played.

Physical Measures

- Controlled entry to buildings.
- Out of hour's security.
- Visitor policy.
- ID badges must be visible at all times (for staff and visitors)**.**

Telephone Calls and Answering Machines

- Verify the details of the caller.
- Obtain their telephone number.
- Provide the minimum information necessary.
- If in doubt of the caller's identity tell the caller that you will ring back.
- When returning the call if possible use a phone number obtained from an independent source.
- Take care when making a phone call that you do not reveal confidential information by being overheard – make confidential phone calls in a separate room.
- If you must leave an answer phone message leave the minimum information necessary.
- Ensure that you replace the receiver correctly after leaving an answerphone message.

- Ensure that you listen to answer phone messages in an environment where they cannot be overheard.

Mobile Devices
The following devices are considered to be mobile devices:

- Laptops
- iPads
- Memory sticks
- Mobile/smart phones

When using an authorised work mobile device you must ensure that it is safe to do so:

- Ensure that the information on the screen is not visible to anyone not authorised to see it.
- Never view confidential information in a public place where it can be seen by members of the public.
- Always lock your device when unattended. Hold down the Windows button and the 'L' button to lock a screen.

Don't share your work mobile devices

- Work issued mobile devices should not be shared with anyone.

When using a Wi-Fi connection

- Stick to using only HTTPS (secure) websites so that your web browsing is encrypted even if it travels over an unencrypted connection. You can check if any web site is using HTTPS by looking for the small padlock by the address bar within your web browser.
- Use NHS provided remote access (VPN, Virtual Private Network) for work purposes when connected to any Wi-Fi; this means that all your network traffic (not just your web browsing) is encrypted.
- If possible, try not to connect to unsecured public Wi-Fi networks - these are often found in hotels, coffee shops and other public spaces. You can confirm if a network is secure when you see a small padlock next to it as you're selecting to potentially join the network.

You should ensure you DO:

- Store work issued mobile equipment securely when not in use on and off site.
- Ensure files containing personal or confidential data are stored on the appropriate shared drive with controlled permissions (need-to-know access).
- Only use NECS approved encrypted memory sticks – available from the IT Help Desk.
- Report any stolen work issued mobile equipment immediately via SIRMS: https://sirms.necsu.nhs.uk/ .
- Understand that the security of your work issued mobile equipment is your responsibility.

You should ensure you DO NOT:

- Disable the virus protection software or bypass any other security measures put in place.
- Leave work issued mobile equipment unattended in a car and/or visible when traveling between locations.
- Leave mobile equipment unattended in a public place e.g. hotel rooms, train luggage racks etc.
- Install or download software onto devices. This should be carried out by IT **only**.

KNOW YOUR RESPONSIBILITIES:

The CCGs IT network is managed on behalf of NHE England by NECS. It is intended to be used for official business and as such, NECS and the CCG reserves the right to monitor activity on all NHSE provided equipment and services, violation of which may result in disciplinary action or criminal/civil proceedings. Under no circumstances are you permitted to use NHSE, NECS or CCG equipment to - Conduct your own business for personal gains - Access create or distribute illegal materials such as child pornography or ethnic hate inducing content, or materials that can be construed as rude, intolerant or demeaning - Share confidential information with any unauthorised party or - Install software without prior NECS IT approval.

The above does not represent the complete list of computer usage violations. For further details, please refer to the NECS IT Acceptable Use Policy, available on the NECS public website or in paper by contacting the NECS IT Service Desk. By reading and acknowledging this handbook you are confirming that you have accepted this information.

Communication via Text

- Ensure that the recipient has consented to receive text communication.
- Ensure that the mobile number is that of the intended recipient.
- Ensure that the content of the message contains the minimum information possible and will not breach confidentiality or contain material that the person may find embarrassing or damaging.

Communication via Post

- Confirm the name, department and address of the recipient.
- Seal the information in a robust envelope, ensure it is correctly addressed (do not use abbreviations) and mark as private and confidential where appropriate.
- Add a return to address to the back of the envelope.
- Where necessary ask the recipient to confirm receipt.

Email

- Staff must be careful when sending emails containing personal identifiable / commercially sensitive information via email.
- The minimum information should be sent via email.
- Both sender and recipient in NHS organisations must have an NHS mail account ending in @nhs.net.
- Organisations can get their email system accredited for security by NHS Digital therefore the landscape is constantly changing.
- Further information is available from NHS Digital here https://digital.nhs.uk/services/nhsmail/the-secure-email-standard
- Care should be taken to ensure that emails are sent / forwarded to the correct recipient.
- Emails should include an appropriate disclaimer:
- **CHECK** any attachments containing personal information before sending and then **CHECK AGAIN** or have someone else check. Most IG incidents are related to the wrong personal information being attached to the wrong email or sent to the wrong place through human error.

KNOW YOUR RESPONSIBILITIES:

Where person identifiable / business sensitive information is required to be sent to an organisation that has no facility to set up a secure encrypted email address the NHS Mail encryption feature can be used:

In the subject field of the email, enter [secure]'before the subject of the message. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets aren't used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment. Further instruction on how to use this feature is available in the NHS Digital document Encryption Guide for NHSmail Version 2.0, October 2016 or from the national NHSmail helpdesk on 0333 200 1133 or email helpdesk@nhs.net

For further information please refer to the North Tyneside CCG Information Security Policy.

14. DATA PROTECTION LEGISLATION

The Data Protection Act 2018 defines UK law on the processing of identifiable data of living individuals. It is a piece of legislation which governs the protection of personal data in the UK. In practice it provides a way for living individuals to control the use of information about themselves.

The Act defines the data protection principles which are listed in Section 2 of this handbook:

The General Data Protection Regulations (GDPR) came into force on 25 May 2018 with the aim of establishing a single legislative regime for data protection

across all EU member states. GDPR will apply in the UK whether we leave the EU or not because it has been established into UK Law via the Data Protection Act 2018. GDPR applies to all public authorities and any organisations processing personal data. The key changes to UK data protection law that the GDPR implemented are as follows:

Data Protection Officer (DPO)
A DPO must be appointed. This may be an existing staff member or may be fulfilled on the basis of a service contract. A DPO must possess in-depth knowledge of data protection/GDPR, be adequately resourced and have clear reporting lines to the most senior management in the organisation. The DPO is an advisory role, not a decision-making role and conflicts of interest must be taken into consideration when appointing. The DPO must be contactable by data subjects.

Your DPO is:

Liane Cotterill

North of England Commissioning Support

Teesdale House

Westpoint Road

Thornaby

Stockton-on-Tees

TS17 6BL

Tel: 01642 745042

Mob: 07796278381
Email: liane.cotterill@nhs.net
Web: www.necsu.nhs.uk

Consent Process
There must be a consent process documented which has regard to the greater restrictions placed on the public sector with regard to its use. The controller must be able to demonstrate that the data subject has given consent to the processing operation. New rules exist where the consent condition is relied upon and the data subject is a child. The CCG will need to be able to obtain and record consent to gather children's data.
Sharing and use of information about individuals within and between partner agencies is vital to ensure co-ordinated and seamless provision of Direct Care to patients. Generally, consent is not required for this purpose under GDPR.

However, the CCG must maintain an awareness of the Common Law Duty of Confidentiality, that if the patient disclosed information in circumstances where it was expected that a duty of confidence applied, it should not normally be disclosed further without the data subject's consent. If this has not been obtained it is the responsibility of the member of staff intending to share personal information to make and document an appropriate decision based on whether disclosure is essential to safeguard either the patient or a third party, is considered to be in the public interest, or there is a legal obligation to share the information (such as a Court Order).

Contracts
GDPR-compliant, binding contracts must in place with data processors and service providers. Controller /processor agreements must stipulate the following:

- Nature of the processing
- Act only on instruction of the data controller
- Confidentiality commitments
- Security measures
- Assist controller with subject rights, security and risk assessment
- Delete or return all personal data to the controller

Changes to Subject Access Requests
Data subjects are given much more control over their personal data under GDPR. Information must be provided to a data subject within 30 calendar days of their request to see it and there is no fee for these services unless the request is manifestly unreasonable. For more information see the Standard Operating Procedure – Subject Access Requests and Subject Rights Requests.

New Right to Restriction
The marking of stored data with the aim of limiting their processing in future. The CCG must be willing / able to respond to data subjects' extended right of restriction of processing where the accuracy of data is contested, processing is unlawful, is no longer needed except for defence of legal claims or where the data subject has objected to the processing pending verification whether the legitimate grounds of the controller override those of the data subject.

New Right to Erasure (right to be forgotten)
The CCG must be willing / able to respond to data subjects' extended right of erasure. Applies where; data is no longer necessary for the purpose, subject withdraws consent, subject objects, data have been unlawfully processed, to comply with a legal obligation, collected in relation to the offer of information society services to a child. There are exemptions (for example, medical history cannot be erased).

New Right to Data Portability
The CCG must be willing / able to respond to data subjects' extended right of data portability. Where processing is done by automated means a subject is allowed to receive his/her own data which he/she has provided to a controller in a structured, commonly used machine-readable format and to transmit it to another controller. Applies only where consent-based or for the performance of a contract.

Extended Right to Object
The CCG must be willing / able to respond to data subjects' extended right to object to processing. Applies where data is processed in the public interest or in the exercise of official authority vested in the controller or the legitimate interests of the controller; a subject may object but it is up to the controller to demonstrate that legitimate interests override the data subject's right to object.

Extended Rights Regarding Automated Decision-making & Profiling
The CCG must be willing / able to respond to data subjects' extended rights in relation to automated processing and profiling. This is a right not to be subject to a decision based solely on automated processing, including profiling. Does not apply where necessary for a contract, is authorised by member state law or is based on the data subject's explicit consent. Special categories (e.g. health) are excluded from automated decision-making or profiling unless there is explicit consent or substantial public interest.

Extended Right to Rectification
The CCG must be willing / able to respond to data subjects' extended right of rectification. This is a right to have inaccurate personal data rectified or have incomplete data completed.

Fair Processing/Privacy Notices
The CCG FPN already includes elements of what is required under GDPR. There are differences according to whether the data has been collected from the data subject or is from another source. A combined list of what must be included is provided below:

- Identity and contact details of the data controller
- Contact details of DPO
- Purpose of processing
- Legitimate interests pursued by the DC
- Recipients of data
- Details where data is transferred to a third country, where applicable
- Categories of personal data processed
- Sources of the data
- Retention period of the data
- Right to request access, rectification, erasure, restriction, objection, portability
- Right to withdraw consent
- Right to lodge a complaint with the ICO
- Existence of automated decision-making, including profiling

NB: Privacy Notices must be written in language understandable by children

Record of Processing Activities
A record of processing activities by controllers must be in place covering:

- Name and contact details of the controller and DPO
- Purposes
- Categories of data subjects and personal data
- Legal basis for processing

- Recipients of the data
- Details where data is transferred to a third country, where applicable
- Envisaged time limits for erasure, where possible
- Technical and organisational security measures
- A record of processing activities by processors must be in place covering:
- Name and contact details of the processor and DPO
- Categories of processing carried out on behalf of each controller
- Details where data is transferred to a third country, where applicable
- Technical and organisational security measures

This could be maintained in the form of an Information Asset Register, including mapping of personal data flows.

Data Protection by Design & DPIA
The CCG must be able to consider data protection in all of its processing activities. Project and change management processes must be in place to actively embed Data Protection Impact Assessment (DPIA) processes. Existing PIA documentation will need to be amended to align with GDPR requirements to contain at least:

- Systematic description of the processing activities and the purposes
- Assessment of the necessity and proportionality of the processing
- Assessment of the risk to the rights and freedoms of the data subjects
- Measures to address the risks

Incident Reporting
Personal data breaches are to be reported by the controller to the ICO within 72 hours after becoming aware, unless the breach is unlikely to result in a risk to the rights and freedoms of a person. Information to be provided will be at least; the nature of the breach, how many people affected, categories of data, name and contact details of the DPO, likely consequences, measures and mitigating actions. A controller must notify a data subject without delay about a breach of their personal data where the breach is likely to result in a high risk to the rights and freedoms of the data subject.

Policies
Existing IG policies have been re-written to take account of GDPR. Non-IG policies which reference the DPA 1998 have been amended in line with GDPR.

15. OTHER RELATED LEGISLATION

You don’t need to be an expert in the law, but you should at least be aware of the legislation and guidance surrounding IG that says how organisations must safeguard information, what processes are in place to use, secure, and transfer information, and how patients and the public have access to personal information. The CCG must comply with the following Laws and Regulations:

- Access to Health Records Act 1990
- Computer Misuse Act 1990

- Common Law Duty of Confidentiality
- Data Protection Act 2018
- Freedom of Information Act 2000
- General Data Protection Regulations 2016
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Human Rights Act 1998
- Records Management Code of Practice for Health and Social Care 2016
- Information: To Share or not To Share (Caldicott2)
- Manual for Caldicott Guardians 2017
- Privacy and Electronic Communications Regulations

16. INFORMATION SHARING

Who can you share information with, and what information can you share? These are not simple questions to answer, but the GDPR and IG are not barriers to appropriate sharing. For example, in 2013 a new Caldicott principle was added that promoted the principle that '**The duty to share information can be as important as the duty to protect patient confidentiality'**. This is the guiding principle when considering the sharing of patient information.

It is important to ensure that there is a balance between sharing information with partners for the purposes of quality of care and keeping information secure and confidential. The CGG must ensure that mechanisms are in place to enable reliable and secure exchange of data within the legal limits.

Guidance on Information Sharing for Safeguarding Practitioners updated by the Department for Education in July 2018 has Seven Golden Rules of Information Sharing which are broadly applicable to all instances of sharing personal and sensitive data:

1. Remember that the GDPR, DPA18 and human rights law are not barriers to justified information sharing, but provide a framework to ensure that personal information about living individuals is shared appropriately.
2. Be open and honest with the individual (and/or their family where appropriate) from the outset about why, what, how and with whom information will, or could be shared, and seek their agreement, unless it is unsafe or inappropriate to do so.
3. Seek advice from other practitioners, or your IG lead, if you are in any doubt about sharing the information concerned, without disclosing the identity of the individual where possible.
4. Where possible, share information with consent, and where possible, respect the wishes of those who do not consent to having their information shared. Under the GDPR and DPA18 you may share information without consent if, in your judgement, there is a lawful basis to do so, such as where safety may be at risk. You will need to base your judgement on the facts of the case. When you are sharing or requesting personal information from someone, be clear of the basis upon which you are doing so. Where you do not have consent, be mindful that an individual might not expect information to be shared.

5. Consider safety and well-being: base your information sharing decisions on considerations of the safety and well-being of the individual and others who may be affected by their actions.
6. Necessary, proportionate, relevant, adequate, accurate, timely and secure: ensure that the information you share is necessary for the purpose for which you are sharing it, is shared only with those individuals who need to have it, is accurate and up-to-date, is shared in a timely fashion, and is shared securely (see principles).
7. Keep a record of your decision and the reasons for it – whether it is to share information or not. If you decide to share, then record what you have shared, with whom and for what purpose.

Staff sharing personal information with other agencies must be aware of the CCG's requirement to have an Information Sharing Agreement in place for the routine sharing of personal data.

Information sharing for non-care purposes

Information that is to be used or shared for non-care purposes, for the benefit of the community, should generally be anonymised. This is defined by the ICO as the process of turning the data into a form which does not identify individuals and where identification is not likely to take place. This may include research, commissioning and assessing the quality and efficiency of services. If the purposes can be achieved with anonymised information then they must be. This means that the information will have all identifiable information that may identify an individual permanently removed from it.

Pseudonymisation within a trusted and safe environment may be an acceptable alternative. This is similar to anonymisation, and is defined by the ICO as the process of giving individuals in a dataset a unique identifier which does not reveal their real identity. Whereas this is still defined as personal data under the Data Protection legislation, its use can help reduce privacy risks by making it more difficult to identify individuals.

If the need to use the information cannot be achieved by either anonymisation or pseudonymisation, then patient consent is generally required. The only exemption to this is if there is an overriding and statutory basis for sharing the information. These include, but are not limited to:

- Compliance with a Court Order
- Notifiable Diseases to Public Health England
- To support the prevention or detection of serious crime
- Under s251 of the National Health Service Act 2006 when ordered by the Secretary of State for Health and Social Care
- NHS Digital has powers to request information which are binding on health bodies, although such powers may not be enforced where a patient has objected

KNOW YOUR RESPONSIBILITIES:

These are complex issues which will typically require expert advice and consideration. Staff faced with decisions on such matters should have regard to national guidance and seek advice from the NECS IG Team.

17. THE NATIONAL DATA OPT-OUT

The national data opt-out is a new service announced on 25 May 2018 by NHS Digital that allows patients to opt out of their confidential patient information being used for research and planning.

Patient information about the programme, including how to set their opt-out choice is available here.

Staff can download leaflets, posters and other resources, including the poster to the left, to use when informing patients here.

The national data opt-out was introduced to allow patients to opt-out from the use of their data for research or planning purposes. This is provided in line with the recommendations of the National Data Guardian, Dame Fiona Caldicott, in her Review of health and social care Data Security, Consent and Opt-Outs. The service is currently in a process of continual development.

By 2020 all health and care organisations will be required to apply national data opt-outs where confidential patient information is used for research and planning purposes. NHS Digital have been applying national data opt-outs since 25 May 2018.

The national data opt-out replaces what were previously known as 'Type 2' opt-out, which required NHS Digital not to share a patient's confidential patient information for purposes beyond their individual care. Any patient that had a Type 2 opt-out had it automatically converted to a national data opt-out from the launch date, and have received a letter with further information.

18. DATA QUALITY

Data quality is vital to the decision-making processes of any organisation. This is particularly important for a public service such as the NHS where financial integrity and public responsibilities of care need to be ingrained in the services provided.

Data Quality can be defined as captured information that is consistently fit for its intended use in representing real world figures and situations to help inform operational decision making and planning, risk assessment and financial transactions.

KNOW YOUR RESPONSIBILITIES:

The aim is for the CCG to hold the most accurate and up-to-date personal information and to make sure that the activity against individuals is recorded correctly.

For more information on Data Quality see the CCG's Data Quality Policy.

19. INFORMATION GOVERNANCE INCIDENTS

It is important that information remains safe, secure and confidential at all times. All staff are encouraged to report all Information Governance related incidents via the Safeguard Incident Reporting Management System (SIRMS). The CCG / NECS can then investigate and learn from those incidents.

Information Governance incidents are categorised as follows (this list is not exhaustive):

- Damage to hard copy records (fire, water)
- Inappropriate access to / disclosure of personal information
- Information left unattended) printer, empty office etc.)
- Lost / stolen equipment paper/hard copy (mobile, USB, laptop)
- Misdirected email received containing confidential information
- Misdirected email sent containing confidential information
- Misdirected hard copy received (e.g. post, fax, etc.)
- Misdirected hard copy sent (e.g. post, fax, etc.)
- Other (IG)
- Password sharing
- Smart card issues

Where any of the above occurs and personal information has been breached outside of the NHS family then the CCG has effectively lost control of that data and this would likely be considered a serious (i.e. Reportable to the ICO) Information Governance incident. If this occurs and you need advice about an incident please contact your line manager or a member of the Information Governance team whose contact details can be found on the final page of this handbook.

KNOW YOUR RESPONSIBILITIES:

The SIRMS system can be accessed by following the link below:
https://sirms.necsu.nhs.uk

Remember that serious (reportable) incidents where personal data has been breached outside of the NHS family must be reported to the ICO within 72 hours. NHS Digital Guidance can be found at the link below:
https://www.dsptoolkit.nhs.uk/Help/29

20. INTRODUCING A NEW PROCESS OR SYSTEM

The ‘project’ could entail:

- The introduction of any new system (electronic or paper) or information technology.
- The introduction of any new service (clinical or non-clinical).
- Any change to the way in which staff collect, record, use, publish or share personal information about patients, staff or members of the public.
- A new policy or procedure.

For any ‘project’ where the processing of personal data is happening it is a legal requirement to conduct a Data Protection Impact Assessment. Even projects that do not include the processing of personal data should at least have a DPIA ‘initial screening’ to make sure. See section 19 below for more information.

21. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

A DPIA is a tool used to identify and then reduce, eliminate or justify any potential risks to the security or confidentiality of personal data within a ‘project’. A DPIA must be carried out at the beginning of any project which involves the collection and use of personal information / sensitive personal information. A DPIA can reduce the risk of harm to data subjects through the misuse of their personal information and ensures that there is a legal basis identified for every instance of processing personal data.

More information can be found on DPIA and how to conduct them via the standard operating procedure: DPIA (Privacy by Design). This also includes the DPIA Template.

A DPIA template can be accessed via the CCG’s shared folder and GP Teamnet.

If you need any advice on a new project or a changing system or process and need help with the completion of a DPIA please contact the NECS Information Governance Team.

KNOW YOUR RESPONSIBILITIES:

All processes involving the high risk processing of personal data must have a DPIA conducted to ensure risks or prevented, reduced, eliminated, or accepted.

Anything with an accepted risk that cannot be mitigated must be reported to the ICO. Speak to the NECS IG Team for more information.

22. FAIR PROCESSING /PRIVACY NOTICE (FPN)

A Fair Processing Notice (FPN) or Privacy Notice is a written statement that individuals are given when information about them is collected. An FPN should include:

- The CCG's identity
- The purpose(s) for which the CCG will process the information
- Any additional information in order to make processing fair and lawful

The CCG's FPN for the public and service users can be accessed via the link below:
https://www.northtynesideccg.nhs.uk/fair-processing-notice/

A FPN relating to staff information is available on the CCG's intranet site via the link below:
https://www.northtynesideccg.nhs.uk/fair-processing-notice/

23. RECORDS MANAGEMENT

Records Management is the process by which an organisation manages all the aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through to their lifecycle to their eventual disposal. Any information held by North Tyneside CCG is only of use if it can be retrieved easily and the data contained within it is accurate and up to date. Staff must feel confident that they know how to access and store information in order for them to carry out their role to the best of their ability.

Manual Records
Manual records when not in use should be stored securely. Confidential information should not be left lying around in accessible areas. When a record has become dormant consideration should be given to the North Tyneside CCG Records Management Policy with regard to retention and disposal.

Electronic Records
Access to all PC's / laptops must be password protected. Passwords should not be shared. Computer screens should not be left on view for the public or staff to view personal or commercially sensitive information. PC's / laptops not in use should be locked by pressing Ctrl, Alt and Delete or logged out of completely. Laptops and hand held devices must be kept secure in a safe environment. USB sticks must not be used for confidential information unless they are encrypted, password protected and approved by the NECS IT team.

Retention and Destruction of Records
Please refer to the retention periods in Annex Three of the IGA Records Management Code of Practice for Health and Social Care:
https://www.gov.uk/government/publications/records-management-nhs-code-of-practice

Where an information asset does not appear in Appendix three of the above Code of Practice then the default position is that records should not be kept longer than necessary for the original purpose for which they were collected.

Confidential records should be disposed of via the confidential waste bins provided.

For further information please refer to the Records Management and Strategy.

KNOW YOUR RESPONSIBILITIES:

Accessing Records

- Patients and staff must be fully informed about how their information may be used.
- There are strict conditions under which personal data may be disclosed.
- Certain disclosures are not allowed without explicit unambiguous consent of the individual.
- Individuals can see and have copies of information held about them, and have errors corrected.
- Personal data should be anonymised wherever and whenever possible
- The legitimate use or disclosure of personal data is not an IG breach.
- Sharing of personal data between organisations can take place with appropriate safeguards
- Personal data must be kept secure and confidential at all times.
- Sometimes a judgement has to be made about the balance between the Duty of Confidence and disclosure in the public interest; and such disclosure must be justified and recorded.
- Under the law, the Police and other law enforcement agencies do not have automatic right to see personal data about patients or staff. They must always provide the lawful basis under which they are requesting the information.

24. SUBJECT ACCESS / SUBJECT RIGHTS REQUESTS

Living individuals have a right under the Data Protection Act 2018 to access personal data about themselves which is held in either electronic or manual form by the organisation.

Subject Access Requests can be made by anyone at any time so it is very important that all staff recognise when a subject access request is being made. Within all applications for access to records the applicant will need to prove their identity.

When a Subject Access Request is received the organisation should acknowledge the request within 2 days and respond to the applicant within 30 calendar days. This can be extended by up to 60 further days if a request is particularly resource intensive or difficult. The clock only starts ticking on Subject Access Requests once the identity of the subject has been ascertained.

Most Subject Access Requests will be dealt with by the IG Team within NECS. Standard operating procedures as set out by the NECS Information Governance Team should be followed.

If you receive a request for access to records, or any queries regarding access to records, the request/query should be immediately forwarded to the Information Governance Team within NECS who will ensure that the request is processed and responded to within the time frame specified by GDPR.

For further information please refer to the North Tyneside CCG Information Access Policy and Subject Access Request Procedure

25. FREEDOM OF INFORMATION ACT 2000

The Freedom of Information Act 2000 is an act of law and gives anyone the general right to request information from a public authority. Pubic authorities include government departments, local authorities, the NHS, councils, schools and police forces. Public authorities must also provide information that is freely available through an approved publication scheme. The North Tyneside CCG publication scheme can be accessed by following the link below:

https://www.northtynesideccg.nhs.uk/contact-us/freedom-of-information/publication-scheme/

A Freedom of Information request must be made in writing (or email) stating what information the applicant requires. The applicant does not have to state that it is a Freedom of Information request or a reason as to why they require the information and requests must be 'requester blind' meaning it does not matter who has made the request.

The law requires North Tyneside CCG to respond within **20 working days** of receipt and staff must ensure that FOI requests are passed on to the NECS FOI team promptly.

It is extremely important that whenever CCG staff are required to provide information as part of the FOI process, this information is provided as soon as possible and without undue delay. FOIs that are not responded to promptly can attract complaints from requesters to the ICO.

Freedom of Information guidance for employees / the public can be found on the North Tyneside CCG website by following the link below:

https://www.northtynesideccg.nhs.uk/contact-us/freedom-of-information/

For further information please refer to the North Tyneside CCG Information Access Policy

26. BUSINESS CONTINUITY

North Tyneside CCG has a Business Continuity Plan (BCP) which describes how North Tyneside CCG will discharge its functions in the event of a major incident that causes serious interruption of business operations.

Business Interruption can be defined as;
'An unwanted incident which threatens personnel, buildings, operational procedures, or the reputation of the organization, which requires special measures to be taken to restore things back to normal'

The four key areas considered are:

- Damage/denial of access to premises;
- Non availability of key staff;
- Loss or damage to other resources;
- Loss/damage to IT or data.

To perform its duty on a day-to-day basis, North Tyneside CCG depends upon a wide range of complex systems and resources, and seeks to maintain a good reputation. Inevitably, there is potential for significant interruption to normal business or damage to the organisation's reputation through loss of those systems and resources. North Tyneside CCG's priorities when faced with a significant interruption (whether actual or impending) will always be to:

- Ensure the safety and welfare of its personnel and visitors;
- Endeavour to meet its obligations under legislative requirements;
- Secure replacement critical infrastructure and facilities;
- Protect its reputation;
- Minimise the exposure to its financial and reputational position;
- Facilitate a return to normal operations as soon as practicable.

The Chief Operating Officer is the person with senior level responsibility for Business Continuity Management. Formal oversight of the CCG BCP arrangements is the responsibility of the CCG Executive Committee.

NECS, as providers of the CCG's IG and IT service also have a Business Continuity Plan and conduct annual data security business continuity exercise in line with the DSP Toolkit.

For further information please refer to the North Tyneside CCG Business Continuity Plan

27. THE INFORMATION COMMISSIONER

The role of the Information Commissioner is to ensure compliance with the Data Protection Act, the Freedom of Information Act and the Environmental

Information Regulations. The Information Commissioner's Office has the power to levy substantial fines and in some cases initiate court proceedings on both organisations and individuals.

The General Data Protection Regulation (GDPR) which was introduced on 25th May 2018 strengthened the ICO's powers to fine companies and organisations. Fines of up to four per cent of global turnover can be issued where a serious breach of data protection law has occurred.

28. THE NECS INFORMATION GOVERNANCE TEAM

Liane Cotterill – 01642 745042
liane.cotterill@nhs.net
Senior Governance Manager

Alan Clement – 0191 375 1769
alan.clement@nhs.net
Senior Governance Officer

Pamela Coxon – 0191 3746051
p.coxon@nhs.net
Information Governance Officer
Newcastle Gateshead, Sunderland and South Tyneside CCGs

Hilary Murphy – 0191 2172625
hilary.murphy2@nhs.net
Information Governance Officer
North Tyneside and Northumberland CCGs

Kieran Williams – 0191 3751761
kieran.williams@nhs.net
Information Governance Officer
North Durham and DDES CCGs

Paul Atkinson – 01642 745581
paulrobert.atkinson@nhs.net
Information Governance Officer
Hartlepool and Stockton-on-Tees (HAST) and South Tees CCGs

SIRMS CONTACT

Wendy Marley – 0191 3744157
wendy.marley@nhs.net
Senior Governance Officer (SIRMS)

Document Management:

Version	Release Date	Author	Update comments	Approval route/date
V1	2015	NECS IG/CCG		Unknown
V2	2016	NECS IG/CCG	Slight updates made to ensure robust IG arrangements	Head of Corporate Services– December 2016
V3	2017	NECS IG/CCG	Updated to incorporate the new General Data Protection Regulation Guidance	Executive Committee – 27/2/18
V4	2018	NECS IG/CCG	Updated to incorporate DPA2018 and new DSP Toolkit requirements	Quality & Safety Commiittee
V5	19/3/2019	NECS IG/CCG	Updated to incorporate DPA2018 and new DSP Toolkit requirements	NT CCG Head of Governance
V6	26/3/2019	NECS IG/CCG	Amendment to job titles and addition of DPO contact details	NT CCG Head of Governance

INFORMATION GOVERNANCE STAFF HANDBOOK AND CODE OF CONDUCT CONFIRMATION SLIP – AN ALTERNATIVE TO SIGNING THIS IS TO ACKNOWLEDGE THE DOCUMENT ON GP TEAMNET.

I confirm that:

I have received my copy of the Information Governance Staff Handbook and Code of Conduct and I understand my Information Governance responsibilities.

Name ……
Signature……..
Job Title……
Workplace……
Date……..

Please tick the boxes below to confirm that you have read and understood the following Information Governance policies and procedures:

☐ Confidentiality and Data Protection Policy
☐ Data Quality Policy
☐ Information Access Policy
☐ Information Governance and Information Risk Policy
☐ Information Security Policy
☐ Records Management Policy and Strategy
☐ Email and Acceptable Use Policy
☐ Social Media Policy
☐ Confidentiality Audit Procedure
☐ Subject Access Request Procedure
☐ Information Labelling and Classification Procedure
☐ Privacy Impact Assessment Guidance

***Please note:** North Tyneside CCGs procedures are available on GP Teamnet and by acknowledging the document on GP Teamnet you are confirming that you have read and understood the above policies and procedures.

Please return to:

Information Governance Team
NHS North of England Commissioning Support Unit
Information Governance Office
John Snow House
Durham University Science Park
Durham
DH1 3YG

Alternatively please email this slip to:

NECSU.IG@nhs.net