Confidentiality: Code of Conduct Policy

Authorship:	Information Governance
Committee Approved:	Integrated Audit & Governance Committee
Approved date:	03/03/2021
Review Date:	2 years from approval
Equality Impact Assessment	**Screening**
Sustainability Impact Assessment	**Completed**
Data Protection Impact Assessment	**Not Required**
Target Audience:	**All Staff**
Policy Reference No:	N/A
Version Number:	2.0

The on-line version is the only version that is maintained. Any printed copies should, therefore, be viewed as 'uncontrolled' and as such may not necessarily contain the latest updates and amendments.

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by & Date	Date on Intranet
0.1	Barry Jackson	First draft for comments	NR	
1.0	Barry Jackson	Approved version		
1.1	Helen Sanderson	Amendments to reflect HSCIC Guidance and Caldicott 2	NR	
1.2	Mark Culling	Amendments to reflect the Data Protection Act 1998 (expected to be superseded by a Data Protection Act 2017 incorporating the requirements of the General Data Protection Regulation).		
2.0	Hayley Gillingwater	Removal of reference to DPA 98 Updates to password guidance. Updates to policy guidance. Updates to Confidentiality Dos & Don'ts. Information on the National Opt-Out	IAGC 03.03.2021	

Contents

1 INTRODUCTION AND APPLICABILITY

The purpose of this Code of Conduct is to lay down the key principles that staff should follow when handling personal confidential/sensitive or corporately sensitive information. All staff should to be aware of their responsibilities for safeguarding confidentiality and preserving information security.

All employees working in the NHS are bound by a legal duty of confidence to protect personal confidential information they may come into contact with during the course of their work. This is not just a requirement under their contractual responsibilities but also a requirement within the common law duty of confidence, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) and in addition, for health professionals through their own professional Codes of Conduct. These responsibilities continue to exist after employment has terminated. It is also a requirement within the NHS Care Record Guarantee, produced to assure patients regarding the use of their information.

This means that employees are obliged to keep any person identifiable information strictly confidential e.g. service user and employee records. Disclosures and sharing of person identifiable information are governed by the requirements of Acts of Parliament and government guidelines. It should be noted that employees also come into contact with non-person identifiable information which should also be treated with the same degree of confidentiality e.g. business in confidence information.

It is important that staff protect personal confidential/sensitive and corporately sensitive information at all times, and must therefore ensure that they are aware of and comply with all information governance policies and complete their statutory and mandatory information governance training.

2 ENGAGEMENT

This policy has been developed based on the knowledge and experience of the Information Governance team. It is derived from a number of national codes and policies which are considered as best practice and have been used across many public sector organisations.

3 IMPACT ANALYSES

3.1 Equality

An equality impact screening analysis has been carried out on this policy and is attached at Appendix 1.

As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share *Protected Characteristics* and no further actions are recommended at this stage.

3.2 Sustainability

A sustainability assessment has been completed and is attached at Appendix 2. The assessment does not identify and benefits or negative effects of implementing this document.

3.3 General Data Protection Regulation (GDPR)

The CCG is committed to ensuring that all personal information is managed in accordance with current data protection legislation, professional codes of practice and records management and confidentiality guidance. More detailed information can be found in the CCGs Data Protection and Confidentiality and related policies and procedures. If you are commissioning a project or undertaking work that requires the processing of personal data you must complete a Data Protection Impact Assessment. Please see the CCG's Data Protection Impact Assessment Procedure and Data Protection by Design & Default procedure available on the website for guidance.

3.4 Bribery Act 2010

The Bribery Act is particularly relevant to this policy. The CCG has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from the Bribery Act 2010. Under the Bribery Act 2010 there are four criminal offences:

•   Bribing or offering to bribe another person (Section 1)

•   Requesting, agreeing to receive or accepting a bribe (Section 2);

•   Bribing, or offering to bribe, a foreign public official (Section 6);

•   Failing to prevent bribery (Section 7).

These offences can be committed directly or by and through a third person and, in many cases, it does not matter whether the person knows or believes that the performance of the function or activity is improper.

It should be noted that there need not be any actual giving and receiving for financial or other advantage to be gained, to commit an offence.

All individuals should be aware that in committing an act of bribery they may be subject to a penalty of up to 10 years imprisonment, an unlimited fine, or both. They may also expose the organisation to a conviction punishable with an unlimited fine because the organisation may be liable where a person associated with it commits an act of bribery.

Individuals should also be aware that a breach of this Act renders them liable to disciplinary action by the CCG, whether or not the breach leads to prosecution. Where a material breach is found to have occurred, the likely sanction will be loss of employment and pension rights.

It is the duty of every member of staff to speak up about any genuine concerns in relation to criminal activity, breach of a legal obligation, miscarriage of justice, danger to health and safety or the environment and the suspected cover up of any of these in the workplace. To raise any suspicions of bribery and/or corruption please contact the Chief Finance Officer. Staff may also contact the Local Counter Fraud Specialist (LCFS) at – Audit Yorkshire on 07872 988939/ email nikki.cooper1@nhs.net or Head of Anti-Crime Services on 07717 356707 / email steven.moss@nhs.net.

The LCFS or Chief Finance Officer should be the contact for any suspicions of fraud. The LCFS will inform the Chief Finance Officer if the suspicion seems well founded and will conduct a thorough investigation. Concerns may also be discussed with the Chief Finance Officer or the Audit & Integrated Governance Committee Chair.

If staff prefer, they may call the NHS Fraud & Corruption Reporting Line on 0800 028 40 60 between 8am-6pm Monday-Friday or report online at www.reportnhsfraud.nhs.uk. This would be the suggested contact if there is a concern that the LCFS or the Chief Finance Officer themselves may be implicated in suspected fraud, bribery or corruption.

4 SCOPE

This policy applies to all staff, CCG Members, temporary staff, seconded staff, contractors and others undertaking work on behalf of the CCG etc.

5 POLICY PURPOSE & AIMS

5.1 Confidentiality Principles

All staff must ensure that the following principles are adhered to:-

• Personal confidential information and corporately confidential information must be effectively protected against improper disclosure when it is received, collected, created, stored, transmitted or disposed of.

• Access to personal confidential information or corporately confidential information must be allocated on a need-to-know basis.

• Disclosure of personal confidential information or corporately confidential information must be limited to that purpose for which the disclosure is required.

• Recipients of disclosed information must respect that it is given to them in confidence and treat it accordingly.

• If the decision is taken to disclose information, that decision must be justified and documented.

• When commissioning new systems or services that will involve the processing of personal data you MUST complete a Data Protection Impact Assessment.

• Where services which need to regularly or routinely share confidential information in order to provide the service must have an information sharing agreement in place, including service user information leaflets and a process to obtain consent for sharing.

• Any concerns about disclosure must be discussed with either your Line Manager or the Information Governance Team.

5.2 Protecting Personal Confidential and Corporately Sensitive Information

1. The CCG is responsible for protecting all the information it holds at all times and must always be able to justify any decision to share information.

2. Personal confidential information, wherever possible, must be anonymised by removing as many identifiers as possible whilst not unduly compromising the utility of data. Appropriate data processing agreements need to be in place to obtain information from the relevant organisations.

3. Access to rooms and offices where terminals are present or personal confidential information or corporately confidential information is stored must be controlled. Doors must be locked with keys, keypads or accessed by swipe card. In mixed office environments measures should be in place

to prevent oversight of personal confidential information or corporately confidential information by unauthorised parties.

4 All staff should clear their desks at the end of each day. In particular they must keep all records containing personal confidential information or corporately confidential information in recognised filing and storage places that are locked.

5 All staff should lock their computer or laptop when away from their desk, (activated by Ctrl+Alt+Del, lock computer)

6 Unwanted printouts containing personal confidential information or corporately confidential information must be put into a confidential waste bin. Discs, tapes, printouts and messages must not be left lying around but be filed and locked away when not in use.

7 Your Contract of Employment includes a commitment to confidentiality. Breaches of confidentiality could be regarded as gross misconduct and may result in serious disciplinary action up to and including dismissal.

5.3 Disclosing Confidential Information

1. To ensure that information is only shared with the appropriate people and in appropriate circumstances, care must be taken to check those people have a legal basis for access to the information before releasing it.

2. It is important to consider how much confidential information is needed before disclosing it and only the minimal amount necessary is disclosed.

3. Information can be disclosed:

- When effectively anonymised.
- When the information is required by law or under a court order. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.
- In identifiable form, when it is required for a specific purpose, with the individual's written consent, with another appropriate legal basis or with support under the Health Service (Control of patient information) regulations 2002, obtained via application to the Confidentiality Advisory Group (CAG) within the Health Research Authority[1].
- In Vulnerable Adults and Child Protection proceedings if it is considered that the information required is in the public or child's interest. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.
- Where disclosure can be justified for another purpose, this is usually for the protection of the public and is likely to be in relation to the prevention and detection of serious crime. In this situation staff must discuss with their Line Manager and obtain approval of the Caldicott Guardian.

4. If staff have any concerns about disclosing information they must discuss this with their Line Manager or the Information Governance Team.

5. The national data opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning. Before you disclose any personal information you must ensure that you have taken into account whether the national data opt-out is applicable. It is not applicable for direct care or for the use of anonymised data. More information can be found at the link below or from your IG lead.

    [Understanding the national data opt-out - NHS Digital](#)

6. Care must be taken in transferring information to ensure that the method used is as secure as it can be. In most instances a Data Sharing, Data Re-Use or Data Transfer Agreement will have been completed before any information is transferred. The Agreement will set out any conditions for use and identify the mode of transfer. For further information on Data Sharing Agreements contact the Information Governance team or see the Information Sharing Protocol.

7. Staff must ensure that appropriate standards and safeguards are in place in respect of telephone enquiries, e-mails, faxes and surface mail.

8. Transferring patient information by email to anyone outside the CCG network may only be undertaken through the NHS Mail system (i.e. from one NHSnet account to another NHSnet account or to a secure government domain e.g. .gov.uk), since this ensures that mandatory government standards on encryption are met. As per the Safe Haven and Email Policies.

    Sending information via email to patients is permissible, provided the risks of using unencrypted email have been explained to them, they have given their consent and the information is not person-identifiable or confidential information.

    Staff should be made aware of the NHS Mail facility that allows personal confidential information to be sent securely to non- NHS Mail addresses and allows the recipient to respond in a secure manner if necessary. This should be used wherever possible when corresponding with none NHS Mail account holders where confidential information needs to be sent.

    Guidance on the use of NHS Secure Mail can be found at: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/dcb1596-secure-email

5.4 Working Away from the Office Environment

1. There will be times when staff may need to work from another location or whilst travelling. This means that these staff may need to carry CCG information with them which could be confidential in nature e.g. on a laptop, USB stick or paper documents, therefore appropriate measures must be taken to protect the information whilst away from organisational premises.

2. Taking home/ removing paper documents that contain personal confidential information or corporately confidential information from CCG premises must only be done by authorised staff and the minimum information taken. Appropriate security measures must be adopted to protect that information whilst away from organisational premises.

3. When working away from CCG locations staff must ensure that their working practices comply with CCG policies and procedures. Any removable media must be encrypted as per the current NHS Encryption Guidance.

4. To ensure safety of personal confidential information or corporately confidential information staff must take reasonable steps to ensure the security of that information whilst travelling and ensure that it is kept in a secure place if they take it home or to another location. Personal confidential information or corporately confidential information must be safeguarded at all times and kept in lockable locations.

5. Staff must minimise the amount of personal confidential information or corporately confidential information that is taken away from CCG premises.

6. If staff do need to carry personal confidential information or corporately confidential information they must ensure the following:

   Any personal confidential information or corporately confidential information must be carried in a suitable lockable container, etc. Prior to taking any information out, staff should consider and remember that they may be personally liable for breaches of the Data Protection Act 2018, the General Data Protection Regulation (GDPR) and their Contract of Employment.

7. If staff do need to take personal confidential information or corporately confidential information home they have personal responsibility to ensure the information is kept secure and confidential. This means that other members of their family and/or their friends/colleagues must not be able to see the content or have any access to the information.

8. Staff must NOT forward any personal confidential information or corporately confidential information via email to their home e-mail account. Staff must not use or store personal confidential information or corporately confidential information on a privately owned computer or device.

9. When you remove equipment and data from NHS premises you are responsible for ensuring its safe transportation and storage as far as is reasonably practical. Computer equipment should be kept out of sight and not be left unattended were possible and when stored in the home, windows and doors should be secured when your home is unoccupied. Computer equipment must be transported in a secure, clean environment and must not be left in a vehicle overnight. You may be held liable if you do not take reasonable precautions.

5.5 Carelessness

1. All staff have a legal duty of confidence to keep personal confidential information or corporately confidential information private and not to divulge information accidentally. Staff may be held personally liable for a breach of confidence and must not:

   • Talk about personal confidential information or corporately confidential information in public places or where they can be overheard.

   • Leave any personal confidential information or corporately confidential information lying around unattended, this includes telephone messages, computer printouts and other documents, and

   • Leave a computer terminal logged on to a system where personal confidential information or corporately confidential information can be accessed, unattended.

2. Steps must be taken to ensure physical safety and security of personal confidential information or corporately confidential information held in paper format and on computers.

3. Passwords must be kept secure and must not be disclosed any other person. Staff must not use someone else's password to gain access to information. Action of this kind will be viewed as a serious breach of confidentiality. This is a disciplinary offence and constitutes gross misconduct which may result in summary dismissal.

   • Passwords should not be written down.
   • Passwords should not relate to the employee or the system being accessed.

- Passwords MUST be changed from default values and should not be easy to guess.
- Passwords should not be shared with colleagues.
- Passwords should not be reused; staff should use a different password for each system.

5.6 Abuse of Privilege

1 It is strictly forbidden for employees to knowingly browse, search for or look at any information relating to themselves, their own family, friends or other persons, without a legitimate purpose. Action of this kind will be viewed as a breach of confidentiality and of the Data Protection Act 2018 and the General Data Protection Regulation.

2 When dealing with personal confidential information or corporately confidential information of any nature, staff must be aware of their personal responsibility, contractual obligations and undertake to abide by the policies and procedures of CCG.

3 If staff have concerns about this issue they should discuss it with their Line Manager or Information Governance Team.

5.7 Confidentiality Audits

Good practice requires that all organisations that handle person confidential or confidential information put in place processes to highlight actual or potential confidentiality breaches in their systems, and also procedures to evaluate the effectiveness of controls within these systems. This function will be coordinated by the Policy Directorate Information Governance team through a programme of audits.

6 IMPLEMENTATION

The policy will be made available electronically to all staff and highlighted to staff through newsletters, team briefings and by managers.

'Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCG's disciplinary procedure'.

7 TRAINING & AWARENESS

Staff will be made aware of the policy via website.

8 MONITORING & AUDIT

Adherence to this policy will be monitored on an on-going basis and breaches may result in disciplinary procedures.

9 POLICY REVIEW

This policy will be reviewed in 2 years. Earlier review may be required in response to exceptional circumstances, organisational change or relevant changes in legislation/guidance, as instructed by the senior manager responsible for this policy.

10 REFERENCE MATERIALS

- NHS Confidentiality Code of Practice
- HSCIC: Code of Practice on Confidential Information
- HSCIC: A Guide to Confidentiality in Health and Social Care
- HSCIC: Sending an encrypted email from NHSmail to a non-secure email address
- Report of the Caldicott2 Review - Information: To share or not to share? The Information Governance Review 2013
- Government Response to Report of the Caldicott2 Review 2013
- National Data Guardian for Health & Care: Review of Data Security, Consent and Opt-outs
- The Independent Information Governance Oversight Panel: Annual Report

ANNEX A: Confidentiality Dos and Don'ts

Do's

- Do safeguard the confidentiality of all personal confidential information or corporately confidential information that you come into contact with. This is a statutory obligation on everyone working on or behalf of NHS.

- Do clear your desk at the end of each day, keeping all portable records containing personal confidential information or corporately confidential information in recognised filing and storage places that are locked at times when access is not directly controlled or supervised.

- Do switch off computers with access to personal confidential information or corporately confidential information, or put them into a password protected mode, if you leave your desk for any length of time.

- Do ensure that you cannot be overheard when discussing confidential matters.

- Do challenge and verify where necessary the identity of any person who is making a request for personal confidential information or corporately confidential information and ensure they have authorisation to access, and a legitimate need to know the information.

- Do share only the minimum information necessary.

- Do transfer personal confidential information or corporately confidential information securely, i.e. use an nhs.net email account to send confidential information to another nhs.net email account or to a secure government domain e.g. gsi.gov.uk.

- Do seek advice if you need to share personal confidential information without the consent of the patient/identifiable person's consent, and record the decision and any action taken.

- Do report any actual or suspected breaches of confidentiality at the earliest opportunity

- Do complete statutory and mandatory training and other training as appropriate.

Don'ts

- Don't share passwords or smart cards, or leave them lying around for others to see or use.

- Don't disclose or share information to someone where there is not a legal basis to do so.

- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds to do so.

- Don't use personal confidential or corporately confidential information unless absolutely necessary, anonymise the information where possible.

- Don't collect, hold or process more information than you need, and do not keep it for longer than necessary.

- Don't attempt to obtain access to personal confidential information or corporately confidential information unless you have a legitimate reason to do so.

- Don't leave confidential messages on answering machines or text patients without their prior consent.

- Don't leave computer equipment or records in a vehicle overnight

Appendix 1 – Integrated Impact Assessment

INTEGRATED IMPACT ASSESSMENT		
Policy/project/function/service	Confidentiality: Code of Conduct Policy	
Date of analysis:	27/01/2021	
Type of analysis completed	Quality	X
	Equality	X
	Sustainability	X
What are the aims and intended effects of this policy/project or function?	The purpose of this Code of Conduct is to lay down the key principles that staff should follow when handling personal confidential/sensitive or corporately sensitive information. All staff should to be aware of their responsibilities for safeguarding confidentiality and preserving information security.	
Please list any other policies that are related to or referred to as part of this analysis		
Who does the policy, project, function or service affect?	Employees	X
	Service users	
	Members of the public	
	Other (please list)	

QUALITY IMPACT							
	Please 'X' ONE for each			**Brief description of potential impact**	**Mitigation strategy and monitoring arrangements**	**Risk 5 x 5 risk matrix)**	
	Chance of Impact on Indicator						
	Positive Impact	**No Impact**	**Negative Impact**			**Likelihood**	**Consequence**
	X	**X**	**X**				
PATIENT SAFTEY							
Patient safety /adverse events		x					
Mortality position		x					
Infection control MRSA/CDIFF		x					
CQC status		x					

NHSLA / CNST		x					
Mandatory/statutory training		x					
Workforce (vacancy turnover absence)		x					
Safe environment	**X**						
Standard & suitability of equipment		x					
CLINICAL EFFECTIVENESS							
NICE Guidance and National Quality Standards, eg VTE, Stroke, Dementia		x					
Patient related outcome measures		x					
External accreditation e.g. professional bodies ie RCN		x					
CQUIN achievement		x					
PATIENT EXPERIENCE							
Will there be an impact on patient experience if so how		x					
Will it impact on carers if so how		x					

INEQUALITIES OF CARE							
Will it create / reduce variation in care provision?		x					
STAFF EXPERIENCE							
What is the impact on workforce capability care and skills?		x					
Will there be a change in working practice, if so, how?		x					
Will there be an impact on training	x			Additional training may be required to ensure all staff understand the policy and their requiremen t to align with it.			
TARGETS / PERFORMANCE							
Will it have an impact on performance, if so, how?		x					
Could it impact on the achievment of local, regional, national targets, if so, how?		x					

QUALITY IMPACT

Analysis Rating (see completion notes)	Red		Red/Amber		Amber		Green	X

Approved by:	Commissioner Lead:		GP lead for E&D:	
	Date		Date	

Local Profile Data

General	North Lincolnshire is predominantly a rural area and neighbours; North East Lincolnshire, West Lindsey, South Yorkshire, Nottinghamshire and the East Riding of Yorkshire. North Lincolnshire is geographically large, although the population is small in comparison with some neighbouring unitary authorities. The latest midyear population estimates for North Lincolnshire estimate that 172,292 people live in the local area (ONS, 2019). This represents more than a 3.5% growth in the resident population since 2010 and an annual growth of about 640 more residents a year. The GP registered population as at April 2020 is 181,658. Nearly half of North Lincolnshire's residents, 48%, live in rural market towns and villages, where much of the recent growth in its older population has occurred. North Lincolnshire is serviced by a medium sized Foundation Trust, NLaG, which operates from 3 sites, Grimsby, Scunthorpe and Goole. Scunthorpe General Hospital services the majority of the population providing a seven day scanning/diagnostic service and a busy emergency centre with around 60,000 attendances every year.
Gender	North Lincolnshire has 50.6% female and 49.4% male population (North Lincolnshire Strategic Needs Assessment 2018, Fingertips Public Health Data).
Race	92.3% of the resident population of North Lincolnshire are "White British" and a further 3.2% are of other White origin (not including Irish and Gypsy Travellers). The proportion of ethnic minorities in North Lincolnshire (4.5%) is significantly lower than that seen in the Yorkshire and Humber region (14.2%) and in England as a whole (20.2%) The area has a relatively small Black and Black African population making up less than 1% of residents More than 53% of the BME communities live in the northern part of Scunthorpe. The largest concentration of BME children is in Scunthorpe North, where they represent more than a fifth of the primary school age population. In North Lincolnshire, unemployment amongst the BME community is more than twice that for the White UK population – 14.5% compared with 5.9% (Annual Population Census, 2012). In 2011, more than 8.1% of all school aged children were from Black and Asian communities, with at least half as many more BME children in reception classes as in Year 11. Adding 'other, (Non UK) White', to the BME total, (including White European) the proportion increases to more than 12%. 95.5% of households all residents had English as their main language, compared to 93.4% in Yorkshire and the Humber and 90.9% nationally. More than 60 identifiable different languages are spoken across North Lincolnshire, the most common being Polish, Lithuanian, Bengali and Portuguese. Based on the latest ONS (2018) predictions, net migration in North Lincolnshire is thought to have been around 590 in 2010 and 712 in 2019. Net migration within

	North Lincolnshire was expected to increase gradually, averaging around 750 people per year over the next 24 years but may be affected substantially by the UK exit from Europe.
Disability	In the last census (2011) 19% of residents identified as having day to day activities being limited either a little or lot (due to impairment or health condition); with approximately 6% of residents being blue badge holders. The Life Opportunities Survey (2011), identified that nearly one third of adults aged 16 and over had at least one impairment and 26% of adults aged 16 and over in Great Britain would be covered by the rights under the provision of the Equality Act. • 23.8% of the working population are EA core or registered as having a work-limiting disability (24,700). This is significantly higher than Yorkshire and the Humber (21.4%) and England (19.4%). • 26.7% of all households in North Lincolnshire have at least one person with a long-term health problem or disability (18,899). • 9.2% of the resident population (an estimated 15,333 residents) stated that their daily activities were significantly limited due to a health condition or disability. • 19.3% of the population had some form of day-today activity limiting disability, compared with 18.9% and 17.6% for Yorkshire and Humber and England respectively. • More women have a disability (24.7%) than men (23.0%). This is broadly significantly higher than national values and higher than Yorkshire and Humber comparator groups. • Figures for August 2017 show 5910 people claiming ESA or IB equivalent equates to 3.46% of the total population, which is lower than Yorkshire and Humber figures (3.65%), and higher than the national rate (3.22%). • In 2017, 3485 (14.3%) of school pupils were identified as having Special Education Needs - this was below the national average (14.4) and higher than Yorkshire and Humber (14.0%). Of the 3485 children receiving SEN support 755 had EHC or SEN plans.6 • According to the Census 2011, the number of residents of North Lincolnshire who stated that their 'Day-to-Day Activities were Limited a Lot' was 14,207, 8.6% of all household residents. This compares to 8.7% regionally and 7.9% nationally. However there is significant difference across the age bands, the older people become the higher the percentage of residents whose activities are limited.
Religion or Belief	• The 2011 census stated that 69% of North Lincolnshire residents identified as having a belief. 66% Christian, 2.6% Muslim and 1.8% other (Sikh, Hindu, Buddhist, Jewish or other). For Christianity, this is higher than the national average but lower for other religions. • 7.1.% of residents do not state their religion and 24% state they are of no religion
Sexual Orientation	There are limited accurate statistics available regarding the profile of the lesbian, gay, bisexual and transgender (LGBT) population in North Lincolnshire, the region, or indeed, across England as a whole. Sexuality as a whole has historically not been included in censes or most other official statistics. However, this continues to change and become integrated within demographic studies. The 2011 census estimated 185 persons in a registered same-sex civil partnership. In the Yorkshire and Humber region 94.4% of survey respondents aged 16 or over identified themselves as heterosexual/ straight. Percentages of people identifying as sexualities other than heterosexual/ straight are broadly similar for the Yorkshire and Humber and all England geographical regions with gay/lesbian being the highest percentage at 1%

Pregnancy and Maternity	Locally, according to the ONS in 2018 there were 1,673 live births registered within North Lincolnshire with 2 registered still births. On a National level, there were 657,076 live births recorded in 2018 compared with 679,106 in 2017. In 2018 339,267 of births were registered born within marriage and 317,809 were registered outside of marriage. Since 2009, there has been a National increase in the number of live births registered within a same sex couples. In 2017 1,137 live registered births were recorded within a same sex marriage, whilst 450 were registered outside of marriage.
Gender Reassignment	No local data available. The Home Office 'Report of the interdepartmental working group on transsexual people' based on research from the Netherlands and Scotland, estimates that there are between 1,300 and 2,000 male to female and between 250 and 400 female to male transsexual people in the UK. However, Press for Change estimate the figures at around 5,000 post-operative transsexual people. Further, GIRES (2008) claims there are 6,200 people who have transitioned to a new gender role via medical intervention and approximately 2,335 full Gender Recognition Certificates have been issued to February 2009.
Marital Status	No local data available. There were 239,020 marriages between opposite-sex couples in 2015, a decrease of 3.4% from 2014 when there 247,372 marriages, and 0.8% lower than in 2013. Marriage rates for opposite-sex couples in 2015 were the lowest on record, with 21.7 marriages per thousand unmarried men and 19.8 marriages per thousand unmarried women. Compared with 2005, marriage rates for opposite-sex couples marrying in 2015 were lower at all ages, except for men aged 65 and over and women aged 55 and over where marriage rates increased. In 2015 there were 6,493 marriages between same-sex couples, 56% were between female couples; a further 9,156 same-sex couples converted their civil partnership into a marriage. In 2015, civil ceremonies among opposite-sex couples decreased by 1.6%, while religious ceremonies decreased by 8.0% compared with 2014. Same-sex couples mostly solemnised their marriages in civil ceremonies; there were only 44 religious ceremonies accounting for 0.7% of all marriages of same-sex couples. In 2015, of all individuals marrying a same-sex partner, 85% were forming their first legally recognised partnership compared with 76% for opposite-sex couples.
Age	Based on 2019 estimates, North Lincolnshire's proportion of older people (pensionable age) represents a higher percentage of the total population (21.3%) than seen in Yorkshire and Humber (18.8%) and England (18.4%). The working age population is less (60.2%) than that estimated in the Yorkshire and Humber region (62.1%) or over England as a whole (62.4%). North Lincolnshire's proportion of children represents a lower percentage of the total population (18.5%) than seen in Yorkshire and Humber (19.1%) and England (19.2%). In 2016, the median age of North Lincolnshire residents was 43.8 years, compared with 40 years nationally. North Lincolnshire already has a larger than average population of people aged 65+, and between 2019 and 2043 the 65+ population is projected to grow by a further 37%. Overall, the latest (2018) projections indicate a rise of 3.3% over the next 24 years, from an estimated 172,607 in mid-2019 to 178,336 in mid-2043. The projected

	increase in population in North Lincolnshire is not consistent across the age bands: the population aged 0-14 is projected to decrease by 12.1% from 30,101 in 2019 to 26,456 in 2043; the working age population is projected to decrease by 4% from 105,855 to 101,786; the 65+ population is expected to increase by 37% from 36,651 to 50,095. This age profile, combined with outward migration of working age adults and rising life expectancy, means that the number of people aged 80+ who are most vulnerable to frailty in older age is increasing faster in North Lincolnshire than nationally.

Equality Data

Is any equality data available relating to the use or implementation of this policy, project or function?	N/A
List any consultation e.g. with employees, service users, Unions or members of the public that has taken place in the development or implementation of this policy, project or function.	
Promoting inclusivity; How does the project, service or function contribute to our aims of eliminating discrimination and promoting equality and diversity?	Equal rights and access for all

Equality Impact Risk Assessment test

What impact will the implementation of this policy, project or function have on employees, service users or other people who share characteristics protected by *The Equality Act 2010*?

Protected Characteristic:	No Impact	Positive Impact	Negative Impact	Evidence of impact and if applicable justification where a *Genuine Determining Reason* exists
Gender (Men and Women)	X			
Race (All Racial Groups)	X			
Disability (Mental and Physical, Sensory Impairment, Autism, Mental Health Issues)	X			
Religion or Belief	X			
Sexual Orientation (Heterosexual, Homosexual and Bisexual)	X			

Pregnancy and Maternity	X			
Transgender	X			
Marital Status	X			
Age	X			

Action Planning

As a result of performing this Equality Impact Analysis, what actions are proposed to remove or reduce any risks of adverse outcomes identified on employees, service users or other people who share characteristics protected by The Equality Act 2010?

Identified Risk:	Recommended Action:	Responsible Lead	Completion Date	Review Date

SUSTAINABILITY IMPACT

Staff preparing a Policy / Board Report / Committee Report / Service Plan / Project are required to complete a Sustainability Impact Assessment. Sustainability is one of the Trust's key Strategies and the Trust has made a corporate commitment to address the environmental effects of activities across Trust services. The purpose of this Sustainability Impact Assessment is to record any positive or negative impacts that this activity is likely to have on each of the Trust's Sustainability Themes.

	Positive Impact	Negative Impact	No Specific Impact	What will the impact be? If the impact is negative, how can it be mitigated? (action)
Reduce Carbon Emission from buildings by 12.5% by 2010-11 then 30% by 2020			X	
New builds and refurbishments over £2million (capital costs) comply with BREEAM Healthcare requirements.			X	
Reduce the risk of pollution and avoid any breaches in legislation.			X	
Goods and services are procured more sustainability.			X	
Reduce carbon emissions from road vehicles.			X	

Reduce water consumption by 2020.			X	
Ensure legal compliance with waste legislation			X	
Reduce the amount of waste produced by 5% by 2010 and by 25% by 2020			X	
Increase the amount of waste being recycled to 40%.			X	
Sustainability training and communications for employees.			X	
Partnership working with local groups and organisations to support sustainable development.			X	
Financial aspects of sustainable development are considered in line with policy requirements and commitments.			X	