Acceptable Computer Use Policy

August 2020

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

If you need this document in a different format or language (e.g. large print, Braille, audio or easy read), please contact us on 01482 344700, or email HULLCCG.contactus@nhs.net, or write to: NHS Hull Clinical Commissioning Group, 2nd Floor, Wilberforce Court, Alfred Gelder Street, Hull HU1 1UY.

Name of Policy:	Acceptable Computer Use Policy
Date Issued:	September 2020
Date to be reviewed:	2 years from approval date

Policy Title:	**Acceptable Computer Use Policy V2.0**	
Supersedes: (Please List)	**Acceptable Computer Use Policy V1.3** **Acceptable Computer Use Policy V1.2**	
Description of Amendment(s):	Transferred to new template Removal of reference to eMBED	
This policy will impact on:	All Staff	
Policy Area:	Information Governance	
Version No:	2.0	
Author:	Information Governance	
Effective Date:	September 2020	
Next Re-publication Date:	September 2022	
Equality Impact Assessment Date:	August 2020	
APPROVAL RECORD		**Date:**
	Integrated Audit and Governance Committee	September 2020
Consultation:	IG Steering Group	August 2020
	Relevant Others	August 2020

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 and Date	Date on website
0.1	Barry Jackson	First draft for comments	NR	N/A
1.0	Barry Jackson	Approved version	IAGC 11/03/14	11/03/14
1.1	Chris Wallace	Updated to include social media	NR	N/A
1.2	Chris Wallace	Amendments based on feedback	IAGC 08/09/15	
1.3	Mark Culling	Amendments to reflect the change from NYHCSU to eMBED Health Consortium IT Systems	IAGC 13/11/18	13/11/18
2.0	Hayley Gillingwater	Removal of eMBED Transferred to new template. Addition of Roles and Responsibilities Video Conferencing Facilities Personal Confidential Data (PCD) definitions.	IAGC 08.09.20	09.09.20

CONTENTS

1. INTRODUCTION

1.1. This Acceptable Use Policy (AUP) applies to any CCG staff or contractors using IT systems, computer equipment and network services. This includes employed staff, temporary staff and contractors granted access, including access to the guest wireless. It is designed to protect the CCG our employees, customers and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

1.2. The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime. Everyone who works at the CCG is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or the Information Governance Team.

1.3. "Systems" means all IT equipment that connects to the corporate network or accesses corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

1.4. 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.

2. SCOPE

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

3. POLICY PURPOSE AND AIMS

3.1 **Internet/Intranet Access**

Access is provided to the internet through a secure gateway operated by The CCG's IT provider operates a secure firewall and a range of technical systems to attempt to reduce the risk posed by hackers, criminals and fraudsters who may attempt to attack our systems. Users are advised that the primary purpose for the provision of the internet service is for work related matters. As a secondary use users are permitted to utilise the system for their own personal use subject to compliance with the conditions set out at point 3.2. In addition users are advised that this personal use is only permitted during break times and is classed as a privilege which can be removed and is also subject to monitoring as set out in

section 10.

3.2 **Social Media**

Social media is the social interaction among people in which they create, share or exchange information and ideas in virtual communities and networks. This has taken on many forms in the last 10 years and includes sites such as Facebook and Twitter. The use of social media is increasing within society and has become a common method for people to communicate with each other. Social media offers great opportunities for organisations and individuals to listen and have conversations with people they wish to influence. The NHS has steadily embraced the use of social media to allow them to better engage with service users. Below are some point to be taken into consideration when using social media for both business and personal purposes.

- Employees are personally responsible for the content they publish on blogs, wikis or any other form of user-generated media. Be mindful that what you publish will be public for a long time. When online, use the same principles and standards that you would apply to communicating in other media with people you do not know. If you wouldn't say something in an email or formal letter, don't say it online.
- Always identify yourself when using social media for work purposes by giving your name and, when relevant, role within the organisation.
- If you are discussing the organisation or organisation related matters in a personal post you should also identify your role within the organisation as above. Write in the first person. You must make it clear that you are speaking for yourself and not on behalf of the organisation.
- If you publish content to any website outside of the organisation that could be perceived to have a connection to the work you do or subjects associated with the organisation, use a disclaimer such as this:
- "My postings on this site reflect my personal views and don't necessarily represent the positions, strategies or opinions of the organisation."
- Respect copyright, fair use, data protection, defamation, libel and financial disclosure laws.
- Don't provide the organisation's or another's confidential or other proprietary information on external websites.
- Do not publish or report on conversations that are private or internal to the organisation (for example, do not quote such material in a discussion forum post).
- Respect your audience. Don't use personal insults, obscenities, or engage in any conduct that would not be acceptable in the workplace. You should also show proper consideration for others' privacy and for topics that may be considered objectionable or inflammatory, such as politics and religion.
- Don't pick fights, be the first to correct your own mistakes, and don't change previous posts without indicating that you have done so.
- If you read something online that you feel is factually incorrect, inaccurate or otherwise needs an official response from the organisation, then you must refer the matter to the Communications Team.
- Personal use of social media should only occur during your own time such as during lunch breaks.
- There are no restrictions on naming the organisation that you work for but it should be considered carefully what is said in regards to your employer.

- If you feel that there is an issue that needs addressing within the organisation then it is advised that you discuss this with your line manager. If this is not appropriate then concerns can be raised through the organisations whistle blowing policy.

Do not post anything that is libellous or that cannot be supported with evidence. Such actions may be seen as bringing the organisation into disrepute and could lead to disciplinary actions.

3.3 **Video Conferencing Facilities**

Microsoft Teams and GotoMeeting are the only video conferencing facilities that the CCG recommends for hosting meetings. Staff can attend meetings hosted by partners on other systems, as long as done so via a web browser, and not a locally installed app

Microsoft Teams:

MS Teams has been made available by NHS Digital to all users with an NHS Mail email account. It has all the required security accreditations for sensitive data. This is the product recommended for organisation and team meetings.

Microsoft Teams is a collaboration tool that combines voice and video conferencing with WhatsApp style chat, instant messaging and collaboration. It is however more secure and is moderated.

Teams is the preferred communication platform for the CCG as it is UK hosted, GDPR compliant, ISO/27001 compliant and provides integration with other CCG software such as Outlook and ultimately Office 365.

To ensure we keep Personal Confidential Data (PCD) secure however, we need your assistance so that Teams is used correctly, both safely and securely.

Therefore you **MUST** adhere to the following:

1. Minimise the use of PCD (Personal Confidential Data). Definition: see Appendix 1.

   - Only send PCD via instant message where absolutely necessary, use NHSMail to NHSMail (nhs.net) in the first instance.
   - If it is essential to send PCD via Teams, then it must only be sent in an encrypted and password protected attachment from a CCG device.
   - However, PCD **can** be safely verbally disclosed during video and voice conferences, but
   - PCD should NOT be openly used if the Teams meeting is being recorded

2. If you choose to access Teams on personal devices then ensure the device meets the following criteria
   - Device is encrypted
   - Device is fully security updated (Patched)
   - Device requires authentication (i.e. 6 Digit PIN, Complex Password, Fingerprint, FaceID)

- Device locks after a maximum 5 minutes of inactivity
- Device is not Jailbroken/Rooted (All restrictions have been removed).
- Device features a manufacturer supported Operating System (still receives security updates)

3. Do not extract or store PCD from Teams on none CCG personal or other electronic storage devices
   - Do not Copy/Paste from Teams to any other application or the device
   - Do not extract files or messages to any other application
   - Do not attach files from Teams to any other application
4. Do not install additional Add-ons or Apps to Teams

Chats:

Microsoft Teams can be used for private 1:1 chats and group chats without the need to create a team. Any instant messages (IMs) received by a user whilst offline will be available next time that user goes online. Conversation history and chats are persistent, meaning conversations remain even after closing the application. Users must not share sensitive information within a chat unless it is intended for all invited participants. Invited participants will be able to read the chat even if they do not join the meeting, or if they have already been disconnected. Use a separate email or Teams chat for private conversations amongst a sub-group of colleagues.

Files use:

When a Microsoft team is created, a SharePoint site is also automatically created. Each channel within that team will correspond to a folder within the SharePoint site. Any files that are shared within a Teams chat or via the channel's files tab is automatically added. Any permissions are translated from the SharePoint site directly to the Teams site. In order to create a new document as a tab, it must first be uploaded otherwise the file will not be available to add.

GotoMeeting:

GoToMeeting is designed to host meetings for multiple users and can support up to 250 participants. This is the preferred system for large formal meetings. GoToMeeting uses robust encryption mechanisms and protocols designed to ensure the confidentiality, integrity, and authenticity for data that is transmitted between the LogMeIn infrastructure and users, and data stored within the LogMeIn systems on behalf of its users for cloud recordings, transcriptions, and meeting notes.

Users of GoToMeeting must adhere to the same principles and rules as set out above for the use of Microsoft Teams.

There is a function in GotoMeeting that allows the organiser to send transcripts of the chat log to the document folders of participants. This function should only be used if there is a requirement to produce Minutes from the logs and should be restricted to relevant participants. Chat logs saved in document folders should be destroyed following approval of Minutes. Unless there is a clear purpose for sending transcripts to participants this function should not be used as it creates unnecessary duplication of information and is at odds with the data minimization principle (Data Protection Act 2018/ General Data

Protection Regulation).

Additional security steps:

- Password protect your meetings
- Lock your meeting once you are in session
- Dismiss any attendees you do not recognize
- Only allow recording access for specific people – If there is no reason to record the meeting DON'T

You can find further guidance at: https://support.goto.com/meeting/help/covid-19-tips-for-staying-secure-using-gotomeeting

Freedom of Information Act 2000 (FOIA)

Please note that all written information in the Chat Facility of Virtual Meetings remains stored within the App and may also be released under The Freedom of Information Act 2000 (FOIA), if requested. As such, all participants should ensure that the language or topics discussed and recorded are professional, appropriate and pertinent to the Agenda.

FOIA, as part of the Government's commitment to greater openness in the public sector, gives the public a right of access to recorded information held by public organisations (subject to exemptions). This right applies to anyone, anywhere in the world, and includes chat logs and minutes from meetings which are subject to FOIA 2000, and may be released if requested, (unless an exemption applies).

3.4 **Inappropriate Use**

Inappropriate Use of Computer/IT Services. The use of computers and internet services in the following types of activities is specifically prohibited

- Illegal, fraudulent, or malicious activities.
- Partisan political activity, political or religious lobbying or advocacy or activities on behalf of organisations having no connection with the CCG.
- Unauthorised fund-raising or similar activities, whether for commercial, personal, or charitable purposes.
- Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
- Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.
- Viewing, damaging, or deleting files belonging to others without appropriate authorisation or permission.
- Attempting to circumvent or defeat security or auditing systems without prior authorisation and other than as part of legitimate system testing or security research. Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

4. IMPACT ANALYSIS / REGULATIONS

4.1 **Equality**

The CCG is committed to designing and implementing services, policies and measures that meet the diverse needs of its population and workforce, ensuring that no individual or group is disadvantaged.

In developing and applying this policy, the CCG will have due regard to the need to eliminate unlawful discrimination**,** promote equality of opportunity**,** and foster good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

Please see Appendix 2 for the full equality impact assessment and findings.

4.2 **Bribery Act 2010**

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware of their duties and responsibilities arising from The Bribery Act 2010. It is therefore, extremely important that staff adhere to this and other related policies and documentation (as detailed on the CCG's website) when considering whether to offer or accept gifts and hospitality and/or other incentives.

If fraud, bribery and corruption are particularly relevant to a policy, e.g. where the policy covers payments, claims, contracts or financial transactions where an individual or company could make a gain and/or cause a loss to the CCG the section should be headed Counter Fraud, Bribery and Corruption and should include a cross reference to the Counter Fraud, Bribery and Corruption Policy.

Please see Appendix 2 for full details.

4.3 **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.

5. NHS CONSTITUTION

5.1 With respect to this policy the CCG supports the Principles of the NHS Constitution as follows:

The NHS aspires to the highest standards of excellence and professionalism in the provision of high-quality care that is safe, effective and focused on patient experience; in the planning and delivery of the clinical and other services it provides; in the people it employs and the education, training and development they receive; in the leadership and management of its organisations; and through its

commitment to innovation and to the promotion and conduct of research to improve the current and future health and care of the population.

6. ROLES / RESPONSIBILITIES / DUTIES

Review and Maintenance -	Senior Information Governance Specialist
Approval:-	Integrated Audit & Governance Committee
Local adoption:-	Line managers (in scope)
Compliance:-	All staff and contractors (in scope)
Monitoring:-	Service Desk, System Engineers, Line Managers

7. IMPLEMENTATION

The policy will be disseminated by being made available on the website 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'.

8. TRAINING AND AWARENESS

Staff will be made aware of the policy via team briefing and inductions. This document will be made available on the website.

9. MONITORING AND EFFECTIVENESS

Users are advised that all computer use, including e-mail and internet access is monitored and that staff are advised that in accordance with the Employment Practices Data Protection Code monitoring of Internet use will take place subject to the following guidance:

- Monitoring and IT Security Audit will be carried out by the Information Governance Team.
- All audits carried out will be documented.
- Monitoring is required to ensure that employees do not breach any regulations (such as those on harassment) which could have a legal impact on the CCG.
- Traffic will be monitored as opposed to content unless there are reasons for doing otherwise.
- The Internet History on a local computer is to be set to retain information for 20 days (this is the default setting). Users are not to clear, delete or otherwise change the settings on the History settings on their PC. Such action may lead to further detailed examination of the system being necessary.
- Inappropriate use of the Internet services may result in either facility being withdrawn and may constitute an offence under the CCG disciplinary code.
- Spot checks will be done as opposed to continuous monitoring.

Investigations:

During an investigation the CCG may need to access an employee's email account.

Employee email, messaging or internet browsing history will only be accessed for management investigation purposes once HR advice has been taken and the decision has been documented. Where possible employees will be consulted before their information is accessed for this purpose. Employees will not be consulted where doing would be likely to prejudice the investigation.

It is recognised that email accounts may contain private personal and sensitive information, employees should make sure all such correspondence is clearly marked, for example saved in a separate folder marked Private. The CCG will ensure steps are taken to maintain a realistic expectation of privacy during an investigation.

Virus Protection.

The CCG's IT provider will ensure that the appropriate technical steps are taken to reduce the vulnerability of the CCG system to attack from computer viruses. Users are expected to play their part by being aware of the problem of viruses and reporting anything they deem to be suspicious to the IT Helpdesk.

10. POLICY REVIEW

This Policy will be reviewed 2 years from the date of implementation. 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.

11. REFERENCES

Organisational Policies:-

- Information Security Policy
- Data Protection and Confidentiality Policy

Further information on the use of social media can be found below:-
Using Social Media – Practical and Ethical guidance for doctors and medical students – British Medical Association
The Nursing and Midwifery Council's social media guidance.
The Royal College of General Practitioners' social media 'highway code'.
The Royal College of Nursing's 2011 congress discussion about social networking sites (social media).
The General Medical Council's social media guidance.
The Health and Care Professions Council social media guidance (PDF).

APPENDICES Appendix 1

Personal Confidential Data (PCD)

Definitions

Personal Confidential Data (PCD) is legally defined in the EU General Data Protection Regulation and the UK Data Protection Act 2018, The two together form the basis for our Data Protection legislation (DPL).

Under the DPL there are two distinct areas that are defined as Personal Data and as Sensitive Personal Data. Both make up that which is defined as Personal Confidential Data.

Personal Data is classed as any information relating to an identified or identifiable natural person. This is supported by detailed by reference to a series of identifiers including name, online identifiers (such as an IP address) and location data.

Sensitive Personal Data: The GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;
- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

These are also referred to as 'special category data'.

Both Personal Data and Sensitive Personal Data are components of PCD. Other areas that are reflected are the NHS Common Law Code of Confidentiality and the Caldicott Principles

Links covering the above can be found here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/

https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/confidential-patient-information

https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx

APPENDIX 2

Please refer to the EIA Overview & Navigation Guidelines located in *Y:\HULLCCG\Corporate Templates and Forms\Equality and Diversity Information* before completing your EIA)

HR / Corporate Policy Equality Impact Analysis:	
Policy / Project / Function:	Acceptable Computer Use Policy
Date of Analysis:	05/08/2020
Completed by: **(Name and Department)**	Hayley Gillingwater Senior Information Governance Specialist
What are the aims and intended effects of this policy, project or function?	The overall purpose of the policy is to set out the CCG's approach to acceptable computer use within the workplace. The policy will also set out guidance to staff and managers about their responsibilities in relation to acceptable computer use.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	Addition of video Conferencing guidelines.
Please list any other policies that are related to or referred to as part of this analysis	Information Security Policy Data Protection & Confidentiality Policy The Health and Social Care Act 2012 Caldicott 2 Principles –To Share or Not to Share? Common Law Duty of Confidentiality HSCIC Guide to Confidentiality in Health and Social Care General Data Protection Regulation (GDPR) (from 25th May 2018) Protection Act 1998 (superseded by GDPR on the 25th May 2018)
Who will the policy, project or function affect?	All staff.
What engagement / consultation has been done, or is planned for this policy and the equality impact assessment?	Planned: All staff Information Governance Steering Group Integrated Audit & Governance Committee

Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs 5. To demonstrate leadership on equality and inclusion and be an active champion of equalities in partnership programmes or arrangements.	The policy does not directly promote inclusivity but provides a framework for the CCG's approach to acceptable computer use within the workplace; ensuring staff are supported by management and health professionals.

Equality Data	
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine *Protected*	Yes ☐ No x Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next

Characteristics – referred to hereafter as *'Equality Groups'.* Examples of *Equality Data* include: (this list is not definitive) 1: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?
(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

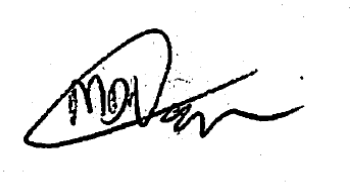
Protected Characteristic:	Neutral Impact	Positive Impact:	Negative Impact:	Evidence of impact and, if applicable, justification where a ***Genuine Determining Reason***[1] **exists (see footnote below – seek further advice in this case)**
It is anticipated that these guidelines will have a positive impact as they support policy writers to complete meaningful EIAs, by providing this template and a range of potential issues to consider across the protected characteristics below. There may of course be other issues relevant to your policy, not listed below, and some of the issues listed below may not be relevant to your policy.				
Gender	x			This policy applies to all regardless of gender.
Age	x			This policy applies to all regardless of age.
Race / ethnicity / nationality	x			This policy applies to all regardless of race/ethnicity/nationality.
Disability	x			This policy applies to all regardless of disability.
Religion or Belief	x			This policy applies to all regardless of religion or belief.

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

Sexual Orientation	x			This policy applies to all regardless of sexual orientation.
Pregnancy and Maternity	x			This policy applies to all regardless of pregnancy/ maternity.
Transgender / Gender reassignment	x			This policy applies to all regardless of transgender/gender reassignment.
Marriage or civil partnership	x			This policy applies to all regardless of marriage or civil partnership.

Action Planning:				
As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?				
Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**
The policy may not be accessible in its current format."	The CCG's Communication Team has developed the 'portal' to signpost individuals to alternative formats.	CCG Communications	Updating of this facility is ongoing	Review September 2022

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:

Signed: Associate Director of Corporate Affairs 
Date: 25.08.20

If you have any comments or feedback about this equality impact assessment, please contact your line manager if you are a member of staff, or telephone 01482 344700, or email HULLCCG.contactus@nhs.net.

Bribery Act 2010:

Under the Bribery Act 2010, it is a criminal offence to:

- Bribe another person by offering, promising or giving a financial or other advantage to induce them to perform improperly a relevant function or activity, or as a reward for already having done so; and
- Be bribed by another person by requesting, agreeing to receive or accepting a financial or other advantage with the intention that a relevant function or activity would then be performed improperly, or as a reward for having already done so.
- Failure to prevent bribery; The Bribery Act also introduced a corporate offence for a relevant commercial organisation (the CCG) to bribe another person intending (1) to obtain or retain business, or (2) to obtain or retain an advantage in the conduct of business. The only defence available to the CCG against Bribery Act offences would be to prove that it had adequate procedures in place designed to prevent persons associated with it from undertaking any of the conduct outlined above.

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 is therefore, extremely important that staff adhere to this and other related policies and documentation (as detailed on the CCG's website) when considering whether to offer or accept gifts and hospitality and/or other incentives.

If fraud, bribery and corruption are particularly relevant to a policy, the section should be headed Anti-fraud, Bribery and Corruption and should include a cross reference to the Local Anti-fraud, Bribery and Corruption Policy. The following wording should also be included:

'If an employee suspects that fraud, bribery or corruption has taken place, they should ensure it is reported to the Local Counter Fraud Specialist (LCFS) and/or to NHS Counter Fraud Authority (NHSCFA) as follows:

- LCFS, AuditOne, Kirkstone Villa, Lanchester Road Hospital, Lanchester Road, Durham, DH1 5RD. Tel: 0191 4415936; Email: counterfraud@audit-one.co.uk or ntawnt.counterfraud@nhs.net
- The CCG's Chief Finance Officer,
- NHSCFA, 0800 028 40 60 (powered by Crimestoppers)
- Online: https://cfa.nhs.uk/reportfraud.'

For further information see http://www.justice.gov.uk/guidance/docs/bribery-act-2010-quick-start-guide.pdf. If you require assistance in determining the implications of the Bribery Act please contact the LCFS on the details above.