# 23 GB Internet Use and E-mail Policy

<table>
<thead>
<tr>
<th>Policy number</th>
<th>23 GB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>3.1</td>
</tr>
<tr>
<td>Approved by</td>
<td>Governing Body</td>
</tr>
<tr>
<td>Name of author/originator</td>
<td>Toni-Dee Downer</td>
</tr>
<tr>
<td>Owner (director)</td>
<td>Elaine Newton, Director of Governance and Compliance</td>
</tr>
<tr>
<td>Date of approval</td>
<td>April 2017</td>
</tr>
<tr>
<td>Date of last review</td>
<td>July 2015</td>
</tr>
<tr>
<td>Review to be completed by</td>
<td>April 2019</td>
</tr>
</tbody>
</table>
## Version control sheet

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>July 2013</td>
<td>Robert Champion</td>
<td>Draft</td>
<td>For consultation</td>
</tr>
<tr>
<td>1.1</td>
<td>July 2013</td>
<td>Robert Champion</td>
<td>Draft</td>
<td>Format changes</td>
</tr>
<tr>
<td>1.2</td>
<td>July 2013</td>
<td>Robert Champion</td>
<td>Final</td>
<td>Approved</td>
</tr>
<tr>
<td>1.3</td>
<td>March 2014</td>
<td>Robert Champion</td>
<td>Draft</td>
<td>Amended to reflect recent guidance on acceptable levels of usage of social networking media. Sections 5.3, 5.4, 5.5 and 5.6</td>
</tr>
<tr>
<td>1.3</td>
<td>April 2014</td>
<td>Robert Champion</td>
<td>Final</td>
<td>For publication</td>
</tr>
<tr>
<td>2.0</td>
<td>July 2015</td>
<td>Toni Downer</td>
<td>Draft</td>
<td>Remuneration Committee and governing Body approved – IG Compliance review required</td>
</tr>
<tr>
<td>2.1</td>
<td>September 2015</td>
<td>Simon Laws, Dan Lo Russo</td>
<td>Draft</td>
<td>Amendments to text re social networking Updates to text regarding NHSmail, CCG intranet, and internet usage (No change to process)</td>
</tr>
<tr>
<td>2.1</td>
<td>September 2015</td>
<td>Toni Downer</td>
<td>Final</td>
<td>No amendments to process. Final for publication</td>
</tr>
<tr>
<td>3.0</td>
<td>December 2016</td>
<td>Toni Downer/Dan Russo</td>
<td>Draft</td>
<td>Amendments suggested from IG Manager and circulated to SPF representatives and Remuneration Committee for final approval</td>
</tr>
<tr>
<td>3.1</td>
<td>January 2017</td>
<td>Toni Downer</td>
<td>Final</td>
<td>Submission to Governing Body for Approval following ratification from SPF and Remuneration Committee</td>
</tr>
</tbody>
</table>
Equality statement

NHS Guildford and Waverley aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. We take into account the Human Rights Act 1998 and promote equal opportunities for all. This document has been assessed to ensure that no employee receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

We embrace the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

See next page for an Equality Analysis of this policy.
Equality Analysis

Equality analysis is a way of considering the effect on different groups protected from discrimination by the Equality Act, such as people of different ages. There are two reasons for this:

- to consider if there are any unintended consequences for some groups
- to consider if the policy will be fully effective for all target groups

Name of Policy: Internet use and E-mail Policy
Policy Ref: 23 GB
Is this New? [ ] Or Existing? [ X ]

Assessment conducted by (name, role):
Toni-Dee Downer, Senior HR Manager
Date of Analysis: 28/12/2016

Directorate: Governance and Compliance
Director’s signature:

Who is intended to follow this policy? Explain the aim of the policy as applied to this group.
All CCG staff and non-employed resources with access to NHS net and CCG network. The CCG’s Internet and Email usage policy is designed to help all staff and non-employed resource understand the CCG's expectations for the use of the Internet, Intranet and email.

Who is intended to benefit from this policy? Explain the aim of the policy as applied to this group.
Policies and procedures apply to conduct on the Internet and whilst using the email system, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of CCG resources, harassment, information and data security, and confidentiality.

1. Evidence considered. What data or other information have you used to evaluate if this policy is likely to have a positive or an adverse impact upon protected groups when implemented?
- Demographic data
- The results of consultations or recent surveys
- Comparison between your policies and functions and similar policies and functions in other public bodies
- Analysis of complaints of discrimination (none received)
- Recommendations of inspection and audit reports

2. Consultation. Have you consulted people from protected groups? What were their views?
The review of this policy has been consulted with Staff Partnership Forum and is in accordance with NHS terms and conditions of employment which is a nationally agreed terms of appointment for NHS staff; therefore this is compliant to all equality requirements.

3. Promoting equality. Does this policy have a positive impact on equality? What
Neutral effect. As detailed in the Equality Statement, policies can be made available in different formats for CCG staff with different communication needs.

### 4. Identifying the adverse impact of policies

Identify any issues in the policy where equality characteristics require consideration for either those abiding by the policy or those the policy is aimed to benefit, based upon your research.

<table>
<thead>
<tr>
<th>a) People from different age groups:</th>
<th>No adverse impact predicted from this policy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>b) Disabled people:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
<tr>
<td>c) Women and men:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
<tr>
<td>d) Religious people or those with strongly held philosophical beliefs:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
<tr>
<td>e) Black and minority ethnic (BME) people:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
<tr>
<td>f) Transgender people:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
<tr>
<td>g) Lesbians, gay men and bisexual people:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
<tr>
<td>h) Women who are pregnant or on maternity leave:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
<tr>
<td>i) People who are married or in a civil partnership:</td>
<td>No adverse impact predicted from this policy.</td>
</tr>
</tbody>
</table>

### 5. Monitoring

How will you monitor the impact of the policy on protected groups?

Complaints made to line managers that are brought to the attention of the Human Resources team.
Contents

1. Introduction and Policy Objective........................................................................................................... 7
2. Core Standards ........................................................................................................................................... 7
3. Scope ....................................................................................................................................................... 8
4. Roles and Responsibilities ....................................................................................................................... 8
   4.1. Managers ........................................................................................................................................... 8
   4.2. Human Resources ............................................................................................................................ 8
   4.3. All employees and all non-employed resources with access: ..................................................... 8
   4.4. The Governing Body and Remuneration Committee................................................................. 9
5. Procedure ............................................................................................................................................... 9
   5.1. Use of the internet ............................................................................................................................ 9
   5.2. Use of Intranet ............................................................................................................................... 11
   5.3. Use of e-mail ................................................................................................................................... 12
   5.4. Use of Social Networking Sites .................................................................................................. 15
   5.5. Liking, Following, Tweeting, Sharing and Retweeting ............................................................... 16
   5.6. Monitoring, Comments and Complaints ...................................................................................... 16
   5.7. Impartiality ...................................................................................................................................... 17
   5.8. Monitoring of e-mail ...................................................................................................................... 17
   5.9. Freedom of Information Act 2000 ............................................................................................... 18
6. References .............................................................................................................................................. 19
7. Approval, ratification and review process ............................................................................................... 19
8. Dissemination and implementation of the Policy .................................................................................. 19
9. APPENDICES ........................................................................................................................................ 21
   9.1. Procedural Document Checklist for Approval ............................................................................ 21
10. Appendix 2 Compliance & Audit Table .............................................................................................. 24
1. Introduction and Policy Objective

1.1. Internet and email is an important part of the CCG’s and the wider NHS communications system. Use of the installed systems/connections is for legitimate CCG business related purposes only and is encouraged to improve the quality of work and productivity in patient care, research, operational matters, education and development. However, we must ensure that the increasing use of information technology maintains patient confidentiality, is not misused, and at the same time is secure and accurate. This policy provides guidance on the CCG’s expectations for staff member’s use of the internet and email.

2. Legislative Framework/ Core Standards

2.1. The CCG’s Internet and Email usage policy is designed to help all staff understand the CCG’s expectations for the use of the Internet, Intranet and email. All existing policies and procedures apply to conduct on the Internet and whilst using the email system, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of CCG resources, harassment, information and data security, and confidentiality. Failure to comply with the requirements of this policy, including non-compliance with the Computer Misuse Act 1990 and Data Protection Act 1998, or infringement of copyright, will be regarded as serious misconduct which will result in disciplinary action being taken. Although each case will be judged on its own merits, misuse of the Internet and/or email (or any misuse of computer systems) may be considered Gross Misconduct and will lead to disciplinary action which may result in dismissal.

Examples of gross misconduct could include:

- Accessing, downloading and/or distributing pornographic or other offensive material. This may include racial, sexual material or derogatory information about others.
- Accessing, downloading and/or distributing information of a discriminatory nature including sexual or racist material or information which is discriminatory towards other groups such as the disabled.
- Deliberately or negligently downloading malware (such as viruses, spyware) which expose undermine the CCG’s IT security measures and expose CCG computer systems and business data to risk of damage or loss.
- Deliberately breaching the Computer Misuse Act 1990 or the Data Protection Act 1998, for example, passing patient related data to inappropriate parties.
• Downloading computer software, storing data (such as music, video files and images) or using copyrighted materials or software without authorisation.
• Administering, supporting or moderating a 3rd party internet site such as discussion groups, fan-sites or websites for a non-CCG business.

3. Scope

3.1. This policy covers all employees within the CCG and all non-employed individuals granted access to our internet, intranet, or email systems and will supersede all other relevant policies under previous terms and conditions of employment held by individuals who have transferred into The CCG from other NHS organisations

4. Roles and Responsibilities

4.1. Managers

4.1.1. Managers are responsible for:
• Maintaining discipline within the organisation and ensuring employees are aware of the standards outlined within this policy.
• Seeking advice from HR or Information Governance Manager in advance of any potential discussions relating to indications of misuse.
• Ensuring that at all times, all employees will be treated with respect by being straightforward, direct and open with them.

4.2. Human Resources

4.2.1. HR is responsible for offering advice to Line Managers and for ensuring that the relevant documentation as outlined in this policy is recorded on the employee’s personnel file.

4.2.2. HR is responsible for supporting the process and advising managers where appropriate and promoting best practice.

4.2.3. HR are responsible for reviewing the content as required, and submitting any recommended updates and/or legislative changes to the remuneration committee for approval and the Governing Body for ratification on a biennially basis.

4.3. All employees and all non-employed resources with access

• Adhering to the CCG’s standards of use outlined within this policy.
• Reporting any concerns to their line managers of any potential misuse outlined within this policy.
• All employees are responsible for their own internet usage and also have responsibility for the emails they send. Employees are asked to be vigilant and report any suspected breaches of this policy immediately to their line manager or to HR as appropriate.
• Should a serious breach of this policy be made by a user, then disciplinary action may be taken and this may include dismissal.

4.4. The Governing Body and Remuneration Committee

4.4.1. The Guildford and Waverley CCG Governing Body is responsible for ensuring that sufficient resources are provided to support the requirements and application of the people management policies across the CCG and that compliance with the necessary legislation and professional conduct is maintained; monitoring the application of policies and outcomes, for equality.

4.4.2. GWCCG Governing Body is responsible for approving the policy and procedure and leading the development of a culture that embraces dignity and respect for all.

4.4.3. The Remuneration Committee will review and approve any recommended changes or updates to this policy biennially, to be ratified by the Governing Body.

4.4.4. Biannual analysis on the implementation of this policy will be provided to the Governing Body.

5. Procedure

5.1. Use of the internet

5.1.1. The Internet is a powerful information acquisition and dissemination tool that provides access to unique resources. The CCG reserves the right to restrict access to materials on the Internet where deemed appropriate, this will include access to pornographic and other sites considered offensive. Any restrictions to material by the CCG shall not be deemed to impose any duty on the CCG to regulate the content of material on the Internet. Furthermore, any lack of restriction does not mean that access to that material is authorised.

5.1.2. Use of the Internet is made available to employees for work duties, work related educational purposes and work-related research purposes. Personal use of the internet is limited to approved breaks and outside of agreed working hours only – employees may not use the internet for personal use otherwise during their normal working hours. While personal use is permitted during the periods mentioned
above, this is only providing that the material accessed is appropriate and not potentially offensive to others. Employees should regard this facility for personal use as a privilege that is only exercised in their own time, without detriment to the CCG, their job, or the work of others and should therefore not be abused.

5.1.3. Excessive or inappropriate use of the Internet, including violation of this policy, may result in disciplinary action being taken and/or removal of facilities. It may also lead to dismissal, and/or notification to the proper authorities for criminal/civil proceedings depending on the level of violation.

5.1.4. The accessing of pornographic and abusive or offensive material, including sites that may constitute unlawful discrimination on the grounds of protected characteristics, is not permitted at any time. Such actions will be regarded as gross misconduct and will result in summary dismissal.

5.1.5. The CCG reserves the right to block access to any sites it feels are contrary to CCG policy or where the amount of data traffic generated adversely affects the CCG’s business use of and access to the Internet. This may include access to social networking sites and heavy bandwidth sites, such as video hosting sites. Employees within the CCG are prohibited from accessing social networking sites using CCG equipment. The only exception to this is where access to such sites is required for business purposes. In these circumstances, appropriate prior approval to access such sites must be sought.

5.1.6. The CCG recognises that employees may wish to access the above type of internet sites outside of the workplace. It is expected however, that any employee who wishes to publish content on such sites must, at all times, conduct themselves appropriately, in a manner consistent with their contract of employment with the CCG, and in a way that does not bring the organisation into disrepute or breach confidentiality. Failure to adhere to this may result in disciplinary action being taken.

5.1.7. Information obtained through the Internet may not be accurate, and the user must check the accuracy, adequacy or completeness of any such information. Furthermore, it is the responsibility of the user when using information obtained from the Internet to be aware of copyrighted material and not utilise copyrighted material for CCG business purposes unless permission has been granted by the publisher.
5.1.8. The threat from viruses and security breaches from the use of the Internet are very real. Users must be aware that information and programmes downloaded from the Internet may contain hidden code capable of destroying data or interfering with the network. Therefore, users must take great care and be vigilant if they are required, as part of their employment, to download or install any executable or programme files from the Internet. Any executable program files not connected with an employee’s duty must not be downloaded. Requests for access to executable or programme files from the Internet should be discussed with the CCG’s Information Governance Manager prior to being referred to the CCG’s ICT service provider. All PC’s accessing the Internet must have virus-checking software, which is installed by the CSU on behalf of the CCG. The use of a ‘firewall’ will protect the CCG from 'cyber attacks' from outside the organisation.

5.1.9. Any users of the CCG Internet connection who supply their personal details, including credit card details, etc., whilst accessing web sites do so at their own risk. The CCG employs security measures to counteract commonly encountered and known malware or attempts to extract personal information but cannot guarantee protection against all threats and therefore the onus is on user vigilance. All users of the CCG Internet connection are forbidden from downloading copyrighted material such as music or software as this is against the law.

5.1.10. Any suspected or actual cyber-attacks or information security incidents relating to internet and email usage will be managed in accordance with the CCG’s Disciplinary, Conduct and Capability Policy and related incident reporting procedures, which are aligned with the requirements of the Health & Social Care Information Centre ‘Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation’. This guidance is available at the following link:


5.2. Use of Intranet

5.2.1. The CCG utilises an Intranet for making information available to our staff. The CCG’s intranet is ‘anonymous N3’ and therefore content uploaded to this is accessible by all organisations which have access to an N3 connection (this includes NHS organisations, private providers of NHS services, and other private companies that provide
services to NHS organisations).

5.2.2. As access to any information uploaded to the Intranet cannot be controlled by the CCG, it is important that no confidential or commercially sensitive information is uploaded to the Intranet. This includes third party personal data (e.g. the names of staff members of other organisations) and that of non-senior CCG employees (e.g. those below Executive Director level). Should confidential or commercially sensitive data be uploaded to the intranet in error this will be investigated and managed in accordance with the CCG’s IG Information Security and IG Incident Reporting procedures.

5.2.3. Internet content is managed by the CCG’s Website Co-ordinator and trained and authorised departmental content managers. Requests for new content to be added or existing content to be amended should be referred to these individuals.

5.3. Use of e-mail

5.3.1. Email access provided by the CCG to all employees, whether this is within the CCG, NHS or with anyone throughout the world, should be utilised as a formal communication system only. The NHS has created a secure infrastructure for the provision of email Services (NHS Net/NHSmail) for use throughout the NHS, which is deemed suitable for the transmission and receipt of patient and other confidential data. The use of personal email accounts or non-NHSmail for the transmission or receiving of patient or other person identifiable data or CCG confidential business data is strictly forbidden and any individuals found doing so will be subject to disciplinary action.

5.3.2. NHSmail service is a secure service, this means that NHSmail is authorised for sending sensitive information, such as clinical data, between NHSmail and:

- NHSmail addresses (i.e. from an '*.nhs.net' account to an '*.nhs.net' account).
- The Health and Social Care Information Centre (*.hscic.gov.uk).
5.3.3. Additionally, NHSmail users can securely exchange sensitive information with users of non-accredited or non-secure email services, for example those ending in .nhs.uk, Hotmail, Gmail and Yahoo. Before attempting to use the encryption feature and sending sensitive data, it is essential the guidance documents (PDF, 371.8kB) are understood by both the NHSmail and non-NHSmail user (PDF, 1.1MB).

5.3.4. Patient identifiable data or confidential business data should never be sent without suitable security being in place, except in very exceptional circumstances, and where a proper risk assessment has been completed by the CCG’s Information Governance Manager, additional security measures have been put in place to protect the data, and the necessary authorisation has been granted by the Caldicott Guardian or the CCG’s Information Governance Sub-Committee.

5.3.5. All users of the NHS Mail system are required to comply fully with the NHS Mail Acceptable Use Policy - a copy of the current version can be found at: http://www.nhs.net. Click ‘Search Directory’ and the Acceptable Use Policy (AUP) can be seen in the bottom left hand corner of the screen. (An NHS/N3 connection must be used).

5.3.6. Data held within the CCG’s email system falls within the scope of the Data Protection Act 1998, and where the emails stored identify living individuals these may be subject to an access to personal data request. The Freedom of Information Act 2000 also applies to data held within the CCG’s email system and therefore this may be subject to review and disclose by the CCG unless a relevant exemption applies.

5.3.7. All employees with access to email will have responsibility for sending their own mails. It is, therefore, imperative that the following guidance is read and understood.

- All employees are prohibited in making (or forwarding) any derogatory remarks about any person or company by email.
- All employees must report any potentially defamatory material to their line manager as soon as it is identified so that steps can be taken to remove it permanently.
- All employees are advised that even deleted items may not be eliminated permanently from the system and may be recovered if required.
- Remarks sent by email can unwittingly cause offence and constitute unlawful discrimination in the form of harassment.
They can also found claims under the sex, race or disability discrimination legislation.

5.3.8. All employees:
- Are advised not to send emails in anger or without thought.
- Are advised against the use of email in confrontational situations or as a substitute for face to face management.
- Are prohibited in sending or forwarding any discriminatory messages, even if intended as a joke.
- Must ensure that their email/Internet usage complies with the CCG’s Dignity at Work policy.

5.3.9. Employees must be aware of the increased risk of confidential information sent by email being misdirected and thus the need to consider the use of a different medium in certain cases. Employees must accept the risk that inbound emails may contain explicit or offensive material that is beyond the control of the employer and the distribution of chain letters, inappropriate humour, explicit language or offensive images is not permitted using CCG resources. Employees must not use email either internally or externally to harass anyone in any manner as laid out in the CCG's Dignity at Work Policy. Employees should avoid ‘flame mail’, where content is abusive towards other individuals, even in response to abuse being directed at them.

5.3.10. All email is automatically scanned for viruses and other malware when it comes into the CCG’s email system. However no measures can be 100% effective and there is still a small risk of such software arriving in a user’s mailbox. If you are suspicious of the subject, source or authenticity of any received email messages, you should not open the email. Please contact the CCG’s Information Governance Manager at the soonest opportunity so they can advise on actions to be taken. Employees have a responsibility to draft all mails carefully, taking into account discrimination, harassment, organisational reputation representation and defamation issues.

5.3.11. Email is an imperfect system, and content can be easily copied, forwarded and archived. There is no guarantee that communications either internally or externally are private or that they will arrive at their destination at a particular time or at all.

5.3.12. NHSmail supports the secure exchange of information and is not designed as a document management system. Deletion of old mails is to be managed by each employee keeping in mind data storage
levels, relevant record retention and destruction requirements, contractual evidence and legal discovery issues.

5.4. **Use of Social Networking Sites**

5.4.1. This section sets out how the CCG will use its social media channels to communicate and interact with public, its patients and key stakeholders and other organisations. Information is provided on news, events, jobs, health promotion activity, public & stakeholder engagement opportunities, and much more. Most online communities have their own rules which we will always follow. The CCG reserves the right to remove any contributions that break the rules of the relevant community, or which are not in line with the general guidelines included within this policy.

5.4.2. We intend to create an environment where people are able to contribute their views without fear of abuse, harassment or exposure to offensive or otherwise inappropriate content, when partaking in social media activity involving or relating to the CCG. When contributing your views please ensure that you:

- Do not provide views, opinions or ‘running commentaries’ on live events such as meeting or conferences, as this implies that you are not directing your energy and concentration on the work matter in hand.
- Ensure that confidential business activities remain so and that no correspondence is entered into that may damage the brand, image and reputation of the CCG, or have potential to bring the organisation into disrepute.
- Protect your personal privacy and that of others by not including personal information in your public posts (such as email addresses, private addresses or phone numbers)
- Make your posts relevant to the issues currently being discussed
- Represent your own views and do not impersonate or falsely represent any other person or organisation
- Do not abuse, harass or threaten others
- Do not make defamatory or libellous comments
- Do not use insulting, offensive or hateful language
- Do not promote commercial interests in your posts
- Do not post content copied from elsewhere, for which you do not own the copyright.

5.4.3. The CCG reserves the right to restrict or remove any content that is deemed in violation of this social media policy or any applicable law. Consideration will also be given to block users that breach these guidelines, without any explanation being given.
5.5. **Liking, Following, Tweeting, Sharing and Retweeting**

5.5.1. The CCG follows or likes people and organisations that provide information relevant to our work; such as central government accounts, local media, charities, patient support groups, our partners, and those whose information we can pass on for the benefit of many people and particularly Guildford and Waverley patients.

- The CCG will not necessarily follow or like individuals, but will focus on correspondence relating to health promotion and awareness.
- The CCG will only take part in conversations that are relevant to the business of the organisation and its role in the health economy.
- Requests to share content with other users will be considered on a case by case basis and will generally aim to respond to requests from stakeholder or partner and not for profit organisations, if deemed appropriate.
- By liking, following or sharing information, the CCG does not necessarily endorse that individual or organisation. However, such activity is intended to be in the best interest of the CCG’s followers.

5.6. **Monitoring, Comments and Complaints**

5.6.1. Communications Staff within the CCG’s Governance & Compliance Department will monitor Twitter and Facebook accounts Monday - Friday 9am to 4pm (except Bank holidays and public holidays).

5.6.2. If individuals or organisations contact the CCG via these channels during these times, they will be replied to, if deemed appropriate, as soon as possible.

5.6.3. Enquirers of the CCG should be advised that the appropriate methods of contacting the organisation for official correspondence or if a query is serious, urgent, or involves personal details, should be via the contact us page on the CCG website: [http://www.guildfordandwaverleyccg.nhs.uk/](http://www.guildfordandwaverleyccg.nhs.uk/)

5.6.4. The CCG welcomes feedback from correspondents. However, it may not able to reply individually to all the messages received. The Communications Team will read all direct messages and replies to posts and ensure that any emerging themes or helpful suggestions are passed to the relevant people at the CCG.
5.6.5. In the event of a concern about something posted on a page that the CCG is responsible for, correspondents should be advised to submit their comments or complaints using the processes outlined on the CCG website. This will ensure that the comment, compliment or complaint is sent to the correct department.

5.7. Impartiality

5.7.1. The CCG must be politically neutral in its communications and therefore cannot comment on issues of party politics. Staff are not permitted to use any of the CCG’s social media channels to promote party political messages or other political content. In the weeks preceding an election - local, general or European – public organisations must not to do or say anything that could be seen in any way to support any political party or candidate. The CCG will continue to publish important service announcements using social media but may have to remove responses if they are overtly party political.

5.7.2. In the interests of commercial propriety and competitiveness the CCG will not honour requests from profit-making organisations except when highlighting joint projects or work commissioned by the CCG.

5.8. Monitoring of e-mail

5.8.1. All employees should be aware that to allow the business of the CCG to continue unhindered, or as part of an investigation, the CCG may require access to an individual’s mailbox, for example; where an individual is away for a period and access is required to correspondence urgently. In such cases the CCG will, where possible, request access from the individual. Where this is not possible access will be granted by the ICT service provider on receipt of a written request authorised by the relevant Executive Director or the Director of Human Resources. When access is given by IT to another employee, an email will be sent to the mailbox owner informing them that access has been granted and to whom and confirming the justification for this. Access will be withdrawn as soon as the information required has been retrieved.

5.8.2. All CCG Internet usage is monitored and in addition the CCG has a system (proxy server and web filtering system) which blocks access to websites it deems inappropriate, or where the use of sites will impact on the business needs of the CCG. This system protects members of staff from accidentally accessing unsuitable websites, and will keep a detailed log of every page visited. The web blocker will block access to millions of sites, it cannot however block every
site deemed inappropriate. The responsibility for accessing inappropriate sites lies ultimately with the user. In addition the system may block sites that are required for legitimate business use. If this happens, users will need to contact the CCG’s ICT Service Desk provider requesting the unblocking the site in writing, citing the business need and providing details of the web site URL. If the CCG becomes aware that an employee (or group of employees) may be misusing their Internet access or email facility in contravention of this policy, steps will be taken immediately to suspend access, and to then consider what the appropriate level of intervention is going to be, with consideration being given to the options below as follows:

- Local action by the ICT provider in conjunction with Information Governance and the HR contact, who will have the authority to seize any appropriate computer hardware and/or to review individual employee’s internet access and emails if it is considered to be appropriate. Employees will generally be informed of the intended actions after their network access has been suspended excepting on advice from NHS Protect, the Local Counter Fraud Specialist or the Police.
- The ICT provider will report to the employee’s line manager on material found on the computer, which contravenes this and any other relevant CCG policy. If the line manager, in conjunction with HR contact, considers that this policy has been breached, they will deal with the matter under the CCG’s Disciplinary, Conduct and Capability Policy. Any information discovered during the CCG’s monitoring of email use and internet access will only be used to investigate a breach of this policy and to pursue any subsequent necessary action, and should not be used for any other purpose.

5.9. **Freedom of Information Act 2000**

5.9.1. The Freedom of Information (FOI) Act gives a general right of access to all types of recorded information held by public authorities. The Act sets out exemptions to that right and places certain obligations on public authorities. Since the 1st of January 2005, anyone, anywhere in the world, can ask the CCG (and it might be your department) for copy of any information which it publishes (some information may be exempt), and they don’t have to give any reason. Therefore the CCG also reserves the right to monitor email usage to ensure that it is able to comply with its obligations under the FOIA, Environmental Information Regulations (EIR), and any other applicable regulations or Codes of Practice.

5.9.2. In response to Freedom of Information Act requests received the CCG may disclose in response to these information held within the CCG’s
email system unless a valid exemption applies. Whilst individuals’ views on the disclosure of this material will be considered, the final decision on the release of this information sits solely with the CCG’s Director of Governance and Compliance in accordance with the CCG’s Policy for the Management of Freedom of Information Act requests.

6. References

6.1. The following references have been used to ensure statutory and regulatory compliance:

- 6.1.1. Previous CCG Internet Use and E-mail Policy (April 2013-June 2015)
- 6.1.2. Equality Act 2010
- 6.1.3. Freedom of Information Act 2000
- 6.1.4. NHSmail
- 6.1.5. Twitter
- 6.1.6. NHS Guildford and Waverley CCG Website
- 6.1.7. The Health and Social Care Information Centre
- 6.1.8. Gov.uk

7. Approval, ratification and review process

This policy will be subject to review every 2 years and at any stage at the request of either management or the consultative committee.

7.1. Human Resources will review this policy, with any recommendations or required changes being presented to the Staff Partnership Forum for consultation, the Remuneration Committee for approval and the Governing Body for ratification.

7.2. At least once a year, analysis on compliance with this policy will be produced by HR in consultation with the provider of the CCG’s ICT Services

8. Dissemination and implementation of the Policy

8.1. This document will be disseminated as follows:

- Copies will be made available on the CCG’s Intranet
- The policy will be brought to the attention of all staff periodically through team brief and ebrief and monitored in line with normal assurance processes.
8.2. Awareness and understanding required on an annual basis for all staff through Appraisal and PDP discussions.

8.3. CCG staff will provide confirmation that they have read IG related policies and procedures and fully understand how these relate to their role within the organisation during the Corporate Induction and annual appraisal (PDP) process.
9. APPENDICES

9.1 Procedural Document Checklist for Approval

<table>
<thead>
<tr>
<th>Procedural document checklist for approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong> Is there a sponsoring director?</td>
<td>Yes</td>
<td>Director of Governance and Compliance</td>
</tr>
</tbody>
</table>

1. **Title**
   - Is the title clear and unambiguous? | Yes |
   - Is it clear whether the document is a guideline, policy, protocol or standard? | Yes |

2. **Rationale**
   - Are reasons for development of the document stated? | Yes |

3. **Development Process**
   - Is the method described in brief? | Yes |
   - Are individuals involved in the development identified? | Yes |
   - Do you feel a reasonable attempt has been made to ensure relevant expertise has been used? | Yes |
   - Is there evidence of consultation with stakeholders and users? | Yes |

4. **Content**
   - Is the objective of the document clear? | Yes |
   - Is the target population clear and unambiguous? | Yes |
   - Are the intended outcomes described? | Yes |
   - Are the statements clear and unambiguous? | Yes |

5. **Evidence Base**
   - Is the type of evidence to support the document identified explicitly? | Yes |
## Procedural document checklist for approval

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are key references cited?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are the references cited in full?</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Are local/organisational supporting documents referenced?</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### 6. Approval

| Does the document identify which committee/group will approve it?    | Yes           |          |
| If appropriate, has assurance been sought?                          | Yes           |          |

### 7. Dissemination and Implementation

| Is there an outline/plan to identify how this will be done?         | Yes           |          |
| Does the plan include the necessary training/support to ensure compliance? | Yes         |          |

### 8. Document Control

| Does the document identify where it will be held?                   | Yes           |          |
| Have archiving arrangements for superseded documents been addressed? | Unknown       |          |

### 9. Process for Monitoring Compliance

| Are there measurable standards or KPIs to support monitoring compliance of the document? | Yes           |          |
| Is there a plan to review or audit compliance with the document?            | Yes           |          |

### 10. Review Date

| Is the review date identified?                                       | Yes           |          |
| Is the frequency of review identified? If so, is it acceptable?        | Yes           |          |

### 11. Overall Responsibility for the
### Procedural document checklist for approval

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is it clear who will be responsible for coordinating the dissemination, implementation and review of the documentation?</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

### Director Approval

On approval, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elaine Newton</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>

### Committee Approval

On approval, Chair to sign and date so it can then be forwarded to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation’s database of approved documents.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phelim Brady</td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2 Compliance & Audit Table

Explain how the procedures will be audited i.e. how you will provide assurance that the policy is being adhered to

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Measurable</th>
<th>Frequency</th>
<th>Reporting to</th>
<th>Action Plan/Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies are approved by the agreed date</td>
<td>100%</td>
<td>Biennial</td>
<td>Remuneration Committee</td>
<td>Policy Database</td>
</tr>
<tr>
<td>Systems in place for:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Distribution (including version control)</td>
<td>Database showing status of HR current policies</td>
<td>Biannually</td>
<td>Remuneration Committee/Governing Body</td>
<td>HR Report</td>
</tr>
<tr>
<td>• Monitoring of Implementation Plan</td>
<td>On internet/intranet site and referenced in Appraisals/PDP</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Timely review of all policies and procedures including equality analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Archiving/Retention/Destruction of policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iterative development of Policy responding to comments received regarding the viability of policy implementation</td>
<td>Number of comments received</td>
<td>Biannually</td>
<td>Remuneration Committee/Governing Body following review with DGC</td>
<td>Action Plan to address comments</td>
</tr>
</tbody>
</table>