Walsall Clinical Commissioning Group

IT Acceptable Use Policy

The Audit & Governance Committee approved this document on:

Date: 20.05.2019
Signed: Chair of the committee
Signed: Designated Senior Officer

Please note that the Intranet version of this document is the only version that is maintained. Any printed versions should therefore be viewed as 'uncontrolled' and may not be the most up-to-date.

Version:	V1.0
Status	Ratified
CCG Lead	Head of Corporate Governance, Sara Saville
Senior Officer responsible	Chief Officer, Simon Brake
Ratified by:	Audit & Governance Committee
Date ratified:	20.05.2019
Date Policy is Effective From	Date of ratification
Review date:	February 2022
Expiry date:	Three years from ratification date
Date of Equality and Diversity Impact Assessment	N/A
Date of Health Inequalities Impact Assessment	N/A
Target audience:	CCG staff and staff working for the CCG
National Documents	
CCG linked documents	
Distribution of the document	Hard copies available at reception, accessible from Website, IG team and IG Newsletter.
Implementation of the document	
Document Control and Archiving	Obsolete or superseded documents will be removed from the intranet and where relevant replaced with an updated version. Previous versions will be archived in the safeguard system in accordance with the Records Management NHS Code of Practice; disposal and retention schedule.
Monitoring Compliance and Effectiveness	
References	

CONTRIBUTION LIST
Key individuals involved in developing the document

Name	Designation
Corporate Governance Manager	Walsall Healthcare NHS Trust
Infrastructure Services Manager	Walsall Healthcare NHS Trust

Circulated to the following for consultation

Name/Committee/Group/	Designation
IG Function Leads	
Audit & Governance Committee	

Comments received from consultation

Name/Committee/Group	Comments

Version Control Summary

Version	Date	Comments on Changes	Author
V0.1	April 2019	Removed Walsall Healthcare NHS Trust. Included Walsall Clinical Commissioning Group. Removed section regarding faxing, as WCCG no longer uses fax. Included printer code. Roles & Responsibilities: Included Data Protection Officer and Head of Corporate Governance. Removed Associate Director of IT, Director of People & Culture and Digital Communications Manager. Updated SIRO.	Serena Ellis Serena Ellis Serena Ellis Serena Ellis Serena Ellis

Contents

1.0 Introduction

1.1 The purpose of this policy and its associated documents is to outline the acceptable use, practices and responsibilities that are expected when Walsall Clinical Commissioning Group (WCCG) staff are provided with computer, storage, data and media devices (including but not limited to computer, tablet, smartphone) to conduct WCCG business or interact with internal networks and business systems.

Failure to comply with this policy may result in disciplinary action being taken, which may result in dismissal or criminal prosecution.

1.2 Statement of Intent

This policy is based on existing good practice used in the NHS and sets out the principles and arrangements that must be adopted by all staff when accessing information systems.

1.3 Scope and limitations

This policy sets out the responsibilities for exercising good judgement regarding the appropriate use of information, all electronic devices and network resources to CCG staff where there is a defined business need in relation to IT applications, including but not limited to the following:

- Email
- Internet
- Remote/Mobile Working
- Devices
- Passwords
- Software
- Copyright
- Equipment
- Printing

This policy applies to all areas and activities of the CCG and to all individuals employed by the CCG including contractors, volunteers, students, and agency Staff.

This policy applies to all equipment that is owned or leased, by the CCG; and also any equipment that is either loaned or donated to the CCG. It also applies to the use of @nhs.net addresses, and NHSmail.

2.0 POLICY AIM

The overall aim of the policy is to ensure CCG Staff operate within the parameters set for acceptable use.

3.0 OBJECTIVES

The policy sets out a framework for the safe, efficient and acceptable use of IT applications.

The CCG recognises the benefits of various technological advances to enable CCG staff to benefit its business objectives provided its reputation; patients and staff are protected from any adverse impacts caused by careless or inappropriate usage.

This policy provides a collection of measures for staff to follow on the acceptable behavior in the use of these.

Under no circumstances are CCG staff authorised to engage in any activity that is illegal while conducting CCG business, utilising CCG owned devices, network or email accounts. This includes, but is not limited to:

- Introduction of malicious software or data into the network or service; i.e. viruses, worms, email bombs etc
- Using a CCG computing asset to actively engage in procuring or transmitting material which is illegal
- Accessing data of which the member of CCG staff is not an intended recipient or logging into a computer or account that the member of CCG staff is not expressly authorised to access
- Execute any form of network monitoring which will intercept data not intended for the member of CCG staff, unless this activity is a part of their normal duty
- Introducing phishing scams to allow untrusted sites access to the CCG's network
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a member of CCG's staff's use of a device, via any means, locally or via the Internet/Intranet

In accordance with the Caldicott Principles, Persona Identifiable Data (PID) must only be sent on a 'need to know' basis and there must be a justifiable reason to send this information.

4.0 DEFINITIONS

Devices	Includes any device that can store images and other information required for the CCG's operational business; i.e. desktop computers. This includes laptops, tablets, personal digital assistants (PDAs), mobile phones/smartphones, as well as digital audio and visual recording/playback devices such as Dictaphones and digital cameras.

Media	Includes any physical items that can store data, images and other information and requires another device to access it i.e. CD, DVD, disc, tape or portable hard drives, USB, memory cards.
Personal Identifiable Data (PID)	Any data which can identify an individual, including but not limited to name, address, telephone number, occupation, date of birth, ethnic group. National Insurance number, NHS number, hospital number or any other information which will allow for the identification of the individual.
Phishing	Phishing is the attempt to obtain sensitive information such as usernames and passwords, often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.
Reasonable use	The test for reasonable use for this policy will be determined by the CCG on a case by case basis.
Shared drive	Sharing a peripheral device (network folder, printer etc.) among several users.
SPAM	Irrelevant or unsolicited junk email.
Social media	Internet platforms such as Twitter, Facebook, YouTube etc. Which allow individuals and organisations to publish and share information and comments online. It is enables individuals to become part of different networks of people with similar interests.
Virtual Private Network (VPN)	Enables users to send and receive data across a shared or public network as if their computing device where directly connected to the private network.

5.0 ROLES AND RESPONSIBILTIES

5.1 Senior Information Risk Owner

The CCGs Chief financial officer is the Senior Information Risk Owner (SIRO). The role of the SIRO is to take ownership of the organisation's information risk policy, act as an advocate for information risk on the Governing Body and provide written advice to the Accountable Officer on the content of the annual governance statement in regard to information risk.

5.2 Medical Director (Caldicott Guardian)

Responsibility for ensuring that all patient related personal data is processed and managed in accordance with the Caldicott Principles. The Medical Director acts as the CCGs Caldicott Guardian with responsibility for patient confidentiality.

5.3 Data Protection Officer

The Data Protection Officer (DPO) whose role it is to identify and mitigate any risks to the protection of personal data, to act in an advisory capacity to the business, its employees and upper management and to actively stay informed and up-to-date with all legislation and changes relating to data protection.

5.4 Head of Corporate Governance

The Head of Corporate Governance supports the Caldicott Guardian and SIRO to ensure the confidentiality and data protection work programme is implemented and provides regular reports to senior management. He/she ensures the CCG adheres to the DPA and GDPR, maintaining notification, developing policies and guidance for staff and providing advice to staff.

5.5 Information Asset Owners

Information Asset Owners are individuals who are responsible for the risk management of their information assets. As such they have to understand what information is held, how it is used/transferred, who has access to it and why, in order for business to be transacted within an acceptable level of risk.

They are therefore accountable for ensuring that information assets have appropriate access controls in place and are used consistently and in line with the CCG's Information Security policy.

5.6 IT Infrastructure Services Manager

Walsall Healthcare NHS Trust's IT Infrastructure Services Manager is responsible for promoting a culture of good IT security within the CCG and developing and maintaining policies, procedures and protocols in compliance with this policy and in accordance with good practice. The Trust's IT Infrastructure Services Manager will be supported by Associate Director of IT.

5.7 Managers

Anyone who has a responsibility for staff must ensure that:

- They advise and inform their team of this policy to increase awareness and understanding
- They approve access to any CCG devices and software based on needs and after carrying out appropriate risk assessments
- They respond to concerns raised in a timely manner
- They maintain complete confidentiality relating to all aspects of investigations and do not mention or discuss such cases with any person not involved

- They maintain complete confidentiality relating to all aspects of investigations and do not mention or discuss such cases with any person not involved

5.8 Staff (including contractors and volunteers)

It is the responsibility of staff to ensure that they are using the services set out in this Policy in an appropriate way. They must:

- Protect their password
- Ensure that all PID is removed from any emails or attachments before sending unless the exceptions are met
- Ensure the use of email is consistent with CCG policy and procedures of ethical conduct, safety, compliance with applicable laws and CCG practices;
- Ensure that they know accurately the contact details of the person(s) they are sending message(s) to;
- Raise any concerns at the earliest opportunity
- Maintain appropriate confidentiality during an investigation
- Report any lost or stolen device immediately to the IT Service Desk and the Information Governance Department
- Ensure adherence to the CCG's policy and associated procedures for Reporting and Managing Incidents
- Ensure that equipment is not left unsecured at any time
- Make sure that the remote equipment provided is regularly connected to the CCG's network for relevant updates;
- Not connect any privately owned equipment to the CCG's network unless prior approval has been given
- Ensure their details are correctly maintained in the phone directory
- Comply with IT software update requests on receiving notification
- Save CCG data on the CCG network (not their local hard drive)
- With the exception of nhs.net accounts, staff are prohibited from using third party email systems to conduct CCG business, or to store or retain email on behalf of the CCG

6.0 POLICY DETAIL

6.1 Email

Email is not a confidential means of communication. The CCG cannot guarantee that electronic communications will remain private. Electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Once an email is transmitted it may be altered. Deleting or recall an email from a CCG staff device will not eliminate it from the various systems across the CCG on which is has been transmitted.

The burden of responsibility for the appropriate use of email lies with the sender of the message.

CCG email accounts must only be used for CCG business, save for the use of CCG email account for personal purposes within reasonable limits which is permitted, provided this does not interfere with the performance of a member of staffs duties. The sending of personal emails must be marked accordingly in the subject field.

The CCG's SIRO has the final decision on deciding what constitutes inappropriate and/or excessive use.

All use of email must be consistent with CCG policies and procedures and in accordance with applicable laws and practice.

All emails, whether work based or personal, are the property of the CCG, not the member of staff. However, the individual Staff member and the CCG will be held jointly liable for communications containing statements about an individual, group or organisation that are proven to be:

- Defamatory
- Blasphemous
- Sexually or racially offensive
- Breach the duty of confidence

CCG staff are prohibited from sending SPAM emails.

CCG staff must not send emails containing profanity as it is potentially offensive and these may be blocked by the CCG's IT system.

Email can be used as documentary evidence in disciplinary proceedings, harassment cases, complaints, libel and legal cases and may be subject to Freedom of Information Act and Subject Access requests.

With regards to the exceptions outlined above, the sending of PID via email is prohibited. CCG staff must check that all PID is removed from any emails or attachments before sending. CCG commercially confidential information must be treated with equal security considerations as PID.

CCG staff are prohibited from using third party email systems such as Google, Yahoo, MSN Hotmail etc. to conduct CCG business, or to store or retain email on behalf of the CCG. Such communications must be conducted through proper channels using CCG approved systems unless the Information Governance Operational Group has approved an exemption.

CCG staff must ensure that they know the email address of the person(s) they are sending a message to and obtain confirmation of receipt of important messages. This is particularly important where messages are sent outside the CCG.

Staff are prohibited from automatically forwarding CCG email to a third party email system. Individual messages which are manually forwarded by the member of CCG staff must

not contain PID or CCG confidential information.

CCG staff must not send email in a manner that deliberately attempts to bypass any system log in or audit functionality or attempt to disguise themselves/their sending address in order to misrepresent any aspect of communication.

Emails, including mailshots, must only be sent to a person or group of people who have an interest in the subject. The use of 'distribution lists' must be treated with caution, particularly if PID information is included in the content.

Third parties receiving an email may choose to treat it as a formal communication, as legally binding as if it had arrived on CCG headed paper. It is therefore essential that CCG staff do not make commitments in an email which exceed their authority or to enter into contracts outside the authority delegated to them by the CCG.

If CCG staff receive suspicious emails, these must be deleted unless the recipient is able to verify with the sender that the email is genuine.

Under no circumstances must CCG staff undertake any further action in relation to suspicious emails (such as opening the email clicking on any embedded links, or attachments, or forwarding it on).

The CCG reserves the right to suspend or remove access, temporarily or permanently, from any member of CCG staff suspected or convicted of misuse. Where a member of CCG staff is identified as potentially being in breach of this Policy, the CCG IT Services Department may be instructed to suspend the email account of that individual, pending further investigation and/or action.

6.2 Internet

The CCG recognises the benefits of the Internet, and electronic communications as valuable business communication tools, which must be used in a responsible, professional and lawful manner and in compliance with the CCG staff Code of Conduct. The CCG allows the use of these facilities provided patients and staff are protected from any adverse impacts caused by careless or inappropriate usage.

Undertaking illegal activities through the CCG's network is prohibited. Each CCG staff member accessing the network bears responsibility for, and consequences of, misuse of their access rights.

CCG material that is not already in the public domain must not be placed on any mailing list, public news group, or such service. If posting of such materials is necessary, it must be approved by the Communications Department.

Access to file downloads may be restricted as necessary by IT Services to ensure network and system security. IT Services may also limit access to content and in order to protect copyright. The CCG has the right to withdraw internet access from any member of staff and globally ban access to any site without warning.

The CCG recognises that social media is a platform which will allow it to interact with stakeholders in order to enhance its profile, provide information about the role and aims of the organisation, make professional and developmental contacts, and to gauge and understand the views of stakeholders such as patients.

The CCG further recognises that social media platforms can benefit staff in building and maintaining professional relationships; establishing or accessing professional networks, seeking advice from forums, and accessing resources for professional development. However, CCG staff must ensure that confidentiality and the reputation of the business are protected at all times.

All staff must ensure that they remain vigilant of the difference between social and professional boundaries by:

- Not posting communication which may constitute threats of violence, bullying, intimidation or exploitation to other persons or property
- Not share confidential information inappropriately
- Not post pictures of patients, people receiving care, or staff
- Not post inappropriate comments about patients, or staff
- Not use social media to build or pursue relationships with patients or service users
- Not post communications which do not fall into the previous categories and which are reasonably considered as being grossly offensive, indecent or obscene
- Avoid making any social media communications which could damage the CCG's business interests or reputation, even indirectly
- Not express opinions on behalf of the CCG via social media, unless expressly authorised to do so by the Head of Communications. Staff may be required to undergo training in order to obtain such authorisation.
- Not post comments about sensitive business-related topics, such as CCG performance, or do anything to jeopardise the CCG's trade secrets, confidential information and intellectual property

- Not include the CCG logos or other trademarks, including photographs within which CCG premises are identifiable, in any social media posting or in their profile on any social media
- Personal use of social media is never permitted during working hours or by means of CCG computer, networks and other IT resources and communication systems

6.3 Remote/Mobile Working

Remote and mobile working are both methods which allow CCG staff to conduct CCG business whilst being off site. Remote working is a method of accessing authorised network files and systems via a dedicated VPN connection, whilst mobile working includes any other work off site. CCG staff undertaking remote and/or mobile working will be restricted to the minimum services and functions necessary to carry out their duties.

CCG staff must ensure that equipment, when used to conduct CCG business, will not be left unsecured at any time. CCG staff are responsible for ensuring that unauthorised individuals are not able to see information or access systems.

VPN tokens must be secured at all times and protected from unauthorised access. Any incident must be reported immediately to the IT Service Desk and raised with the Information Governance Department.

Use of any information or devices off site must be for authorised work purposes only. Authorisation is to be obtained from the CCG staff member's line manager following a risk assessment.

If equipment is being used outside of its normal location and might be left unattended, the member of staff is responsible for securing it by other appropriate means.

Staff using mobile devices such as laptops are prevented from transferring confidential data as these do not have external device connectors installed.

Save for any exception approved by the SIRO all CCG IT portable equipment (i.e. a laptop, smart phone or tablet device) must be encrypted with CCG approved software before any information is stored. Where CCG staff have been supplied with such equipment they are responsible for ensuring that it is regularly connected to the CCG network for upgrade of anti-virus software. Before equipment is returned CCG staff must ensure any data is removed.

CCG staff are only permitted to connect non-standard devices to the network via secure method following consultation with IT Services and an approved risk assessment.

All confidential documentation, whether in paper or electronic format must be stored in a secure area when off site, and stored securely during transit.

All CCG management incidents involving the use of remote working facilities must be reported in accordance with the procedure for the reporting and management of incidents; including serious incidents requiring investigation.

Timely incident reporting is crucial to minimise the risk of data loss. All lost or stolen devices must be reported to the IT Service Desk. Where possible, the IT service desk will employ remote wipe technology to remotely disable and delete any data stored when these devices are reported lost or stolen.

Devices required for remote and mobile working are provided to CCG staff subject to management approval. Where these are issued, family members or other acquaintances must not be permitted access to the equipment or data.

Any device used for remote and mobile working must be connected via a secure network.

Whilst offsite if CCG staff decide to use any non- CCG devices for CCG business, under no circumstances must they save PID, confidential, or commercially sensitive information to these devices. CCG staff are responsible for ensuring that such devices have the relevant

security configuration, including up to date anti-virus software.

6.4 Devices

CCG staff are responsible for their use of devices and connections and must take full responsibility for the security and protections of their devices and any information stored on the device. All assigned devices remain the property of the CCG and must be returned on termination of employment with the CCG or on the instruction of a manager.

Returned devices will be wiped of any data by IT Services.

CCG staff must not connect any non- CCG data devices to the CCG network or computers.

Staff must not use the SIM card provided to them with any device other than the one issued with the SIM card without prior approval from IT Services.

Only CCG approved secure data devices or applications must be used for the transfer of PID, confidential, or commercially sensitive data between computer systems when transfer via the CCG network is not possible. This data must not be transferred onto non-approved devices or networks. Data devices must not be used for data storage.

If travelling abroad for CCG business, staff must notify their line manager and IT Services prior to travel to ensure services will be available and that appropriate tariffs are in place.

6.5 Passwords

All systems and devices will be password protected to prevent unauthorised use. Passwords must be changed on a regular basis or when prompted to do so.

Passwords and Smartcards must not be shared. The unauthorised access of passwords and/or smartcards must be reported immediately to the IT Service Desk and an incident must be raised with the Information Governance team in line with the CCG's Incident Reporting Policy/Procedure.

If a member of CCG's staff believes, or suspects, that another person is aware of their password, this must be changed immediately and IT Services informed. CCG staff must not attempt to remove or bypass the password protection.

CCG staff must not add additional password or security measures to any PC or files without first consulting with IT Services.

CCG staff must not leave any device unattended without activating password protections (either by logging out, activating a password protected screensaver or locking the device). CCG staff who discover an unattended device where a previous member of CCG staff has left their access open, must log out from the session or lock it before commencing their own session.

Upon discovering an unattended and unlocked device, the member of CCG staff discovering the breach must follow the Procedure for Reporting and Management of Incidents; including serious incidents requiring investigation. If the breach involves PID, the Information Governance Department must be informed immediately.

Any actions undertaken using another CCG staff's user identity will be assumed to be those of the account owner.

6.6 Software

CCG provided software is only for the purposes of conducting CCG business and bound by the vendor's licence agreements. All business software on a device must either be provided and installed by IT Services or approved for download by the CCG. Under no circumstances must unapproved software be installed.

CCG staff must comply with any requests from IT to update software to ensure device security within 24hours of receiving a notification.

Any CCG staff being aware of, or suspecting, a security breach must immediately alert IT Services and the Information Governance team who will initiate investigative procedures.

6.7 Copyright

All staff must be aware of copyright protection when distributing articles or other third party original work by email, or by posting it on the internet. This includes any form of media licenced solely for use by the CCG for CCG business.

Copyright protection is afforded as soon as any of the following is created:

- original literary, dramatic, musical and artistic work including illustration and photography
- original non-literary written work, e.g. software, web content and database
- sound and music recordings
- film and television recordings
- broadcasts
- The layout of published editions of written, dramatic and musical works

6.8 Equipment

Occasionally, suppliers may want to provide the CCG with free or new leased IT equipment. Staff must ensure they obtain appropriate authorisation first before accepting such offers and consult with IT Services.

CCG staff must contact IT Services if they wish to move or dispose of IT equipment, including donated and leased equipment.

6.9 Printing

Printing PID must only be undertaken as an absolute necessity, and a print code must be used when printing at all times. Staff must further take responsibility in ensuring that information is collected from the equipment immediately and destroyed in line with CCG policy.

If you are issued a Laptop or mobile devices it should only be used by you and not shared with or used by anyone else, including your work colleagues.

Do not connect privately owned or non NHS devices or use such devices with your NHS IT equipment or install unapproved or privately owned software on NHS IT equipment.

You must ensure that any device lost or stolen is reported immediately to your local Security Team.

7.0 Appendix 1: Acceptable Use – User Guide

General

Information technology resources, such as PCs, laptops, Smart Phones and Tablet devices offer new and exciting ways of working and engaging with our colleagues and patients. However, we must also be aware that improper use can impact us, our colleagues, patients, the reputation of the NHS and the public purse.

You will only be given access to systems and information that you require to carry out your work. Accessing or attempting to gain access to systems or information for which you have no 'Need to Know' or 'Need to Use', could be deemed a disciplinary offence.

In line with your organisational policies as well as legal and statutory requirements, you must always ensure that you adequately protect the confidentiality and integrity of any system or information you have been authorised access to. This includes protection against access by unauthorised persons.

Further guidance can be gained from your local Security Team and your Line Manager.

Protection of Systems

You should avoid eating or drinking in the vicinity of any IT equipment. Spilling drinks or food on to keyboards, monitors or other IT equipment could cause serious damage. You should avoid exposing IT equipment to anything that may damage or prevent normal operation, such as: sudden impacts, excessive change in temperatures or humidity.

Only authorised IT support personnel are allowed to open or move IT equipment or reconfigure or change system settings. You could cause serious damage if you attempt this yourself.

When left unattended, even for a short period, you should ensure that you lock your terminal/workstation/laptop/mobile device (using the Ctrl-Alt-Delete function or other applicable method). If left unattended in semi-controlled areas such as conference centres or customer offices or in the office overnight, laptops must be locked to a fixed point using a physical lock available from IT support.

You must ensure that you never leave portable equipment unattended in airport lounges, hotel lobbies and similar areas as these areas are insecure. Although it should be avoided, if you have to leave portable equipment in parked cars, you must ensure it is completely invisible from outside the vehicle and protected from extreme temperatures. When traveling by air, you must ensure that Portable equipment is carried as hand or cabin luggage at all times and not checked in to the hold.

If you are issued a Laptop or mobile devices it should only be used by you and not shared with or used by anyone else, including your work colleagues.

Do not connect privately owned or non NHS devices or use such devices with your NHS IT equipment or install unapproved or privately owned software on NHS IT equipment.

You must ensure that any device lost or stolen is reported immediately to your local Security Team.

Internet Acceptable Use

Internet access via the NHS infrastructure is provided for business purposes to simplify everyday tasks. Limited private use, such as access to web banking, public web services and phone web directories is accepted but excessive personal use of the Internet during working hours should be avoided.

You should not use NHS systems to access the Internet or use your NHS e-mail address for private business activities (such as eBay or auction sites), downloading software, images, music and videos or for personal financial advantage or for private social media and discussion forums.

Work Email Acceptable Use

Email services are provided to you for business purposes. Limited private use for the purpose of simplifying everyday tasks is accepted but private emails should be distributed via web based email services. Private emails should be stored in a separate folder named '*Private e-mail box*'. If retrieval of business emails is required (due to sick leave etc.) this folder will not be subject to inspection. Private emails should be deleted as soon as possible in order to limit storage requirements for non-business information.

You should not use external, web-based e-mail services (e.g. hotmail.com) for official or NHS business communications and purposes.

You must not distribute content that might be considered discriminatory, offensive, derogatory, abusive, indecent, pornographic or obscene, distribute statements of a political or religious or of a personal nature or engage in any illegal activities via e- mail.

Misuse of Information Systems

The use of NHS information or systems for malicious purposes or other than they were intended for could be deemed a disciplinary offence. This includes but is not limited to:

- Attempts to access external or internal systems you are not authorised for.
- Making discriminatory (on the grounds of sex, political, religious or sexual preferences or orientation), or derogatory remarks or accessing such material; this includes but is not limited to sending offending material as embedded or attached information in e-mails or other electronic communication systems
- Acquiring or sending pornographic or material identified as offensive or criminal

- Violating copyright or intellectual property rights, including use of obviously copyright-violated software
- Accessing or attempting to access medical or confidential information without a legitimate purpose and prior authorisation