REMOTE ACCESS AND INFORMATION SECURITY PROCEDURES

Contents

Introduction .................................................................................................................................................. 1
Remote Access ........................................................................................................................................ 2
Access Control ....................................................................................................................................... 2
   Risks resulting from remote access .................................................................................................. 2
   Key Risks – logical ............................................................................................................................ 2
   Key Risks - physical .......................................................................................................................... 3
   Access restrictions ............................................................................................................................ 3
   General Access Guidelines ............................................................................................................. 4
Security Measures .................................................................................................................................. 4
   Personal and confidential data storage and use ............................................................................. 4
   Physical ............................................................................................................................................. 5
   Incident reporting ............................................................................................................................. 6
   Secure disposal and reuse ................................................................................................................ 6
   Best practice ..................................................................................................................................... 6
Contracts of Employment .................................................................................................................... 7
Security Control of Assets .................................................................................................................... 7
Clinical Quality ..................................................................................................................................... 7
   Projects involving patient identifiable data .................................................................................. 7
Procurement of Information Systems and Change Control ................................................................. 8
Information Security Training ............................................................................................................. 9
Appendix A – Legislative Framework ................................................................................................. 10

Introduction

This document accompanies the Remote Access and Information Security Policy and provides guidance on accessing information remotely and in a secure manner. It details risks involved, ways to mitigate potential issues, and outlines good practice for ensuring RCOG information is protected.

Together with the information governance policy suite, RCOG is obliged to abide by all relevant UK and
European Union legislation (See Appendix A for details).

**Remote Access**

Remote access is available to Staff through Citrix, Outlook Web Access and a mobile device app. Emails may also be available on mobile phones and tablets subject to specific security requirements.

**Access Control**

In order to protect RCOG information, staff need to be aware of potential risks associated with remote access and how to reduce that potential.

**Risks resulting from remote access**

RCOG accepts that connections of this nature may introduce risks that may have a serious adverse impact, such as (this list is not exhaustive):

- Unavailability of networks, systems or target information;
- Degraded performance of remote connections;
- Loss or corruption of sensitive data;
- Loss or damage to equipment;
- Breach of legislation or non-compliance with regulatory or ethical standards.

RCOG will implement appropriate controls to manage the risks resulting from the facilitation of remote access effectively.

**Key Risks – logical**

**Loss or theft of devices.** You must report the loss or theft of any IT equipment provided to you by RCOG or any devices holding RCOG data immediately through processes outlined in the RCOG’s IG Security Incident Reporting Policy. It is the user’s responsibility to secure access to this equipment at all times, for example by keeping it in a locked drawer or the boot of a car and out of sight when not in use. This includes but is not limited to smartphones, USB keys and other portable data storage media. Laptop should be encrypted to prevent data access if the device is lost. The IT team can provide guidance and support on encryption.

**Risk of ‘data leakage’ from RCOG.** Users of the system must not download and save any personal or confidential information to the local hard drive or desktop of ANY PC/laptop/tablet/smart phone or ANY removable media device (such as USB thumb drive). **Non-confidential** documents can be saved to a local hard drive or desktop for the purposes of modification and then saved back to a secure RCOG drive (R: or NGA:). Any documents modified on a non-RCOG PC/laptop/tablet/smart phone should be deleted from the device (including the recycle bin) at the end of the work session i.e. not saved permanently on the non-RCOG device.

**Risk of virus infection.** You must not access RCOG systems if the PC/laptop you are using does not have an approved and up-to-date anti-virus product installed. The IT team can provide guidance and
support on the most appropriate products. There can be no exceptions to this rule, as one unprotected PC/laptop gaining access to the network could put the whole RCOG at risk of virus infection.

**Risk of unauthorised access.** Any staff member using the remote access system does so on the condition that they do not share their login details with any other individual.

**Security of data.** When working on mobile devices connected to RCOG’s network either directly (Wifi or cable) or via remote services over the internet all data should be stored on the R: or NGA: drive in the usual way. This way data will be secure and backed up in the event of loss or failure of the device. If you need to work offline then you should backup your work either to the network when you are next connected or to a secure external media device such as an RCOG-provided encrypted USB key. Personal and confidential information should never be stored on unencrypted devices.

**Unauthorised access to and tampering with a laptop, tablet or mobile device,** particularly if there are repeated opportunities for access, may:

- Lead to continuing (and undetected) compromise of information on the device itself;
- Undermine security measures (including the encryption) intended to protect information on the device in the event of loss or theft; and
- Lead to compromise of the systems to which the device is connected, for example, RCOG’s networked systems that are accessed from the device under an approved remote access arrangement.

**Key Risks - physical**

**Loss, theft or damage of hard copy information.** You must report the loss or theft of any document or file immediately, following the IG Security Incident Reporting Procedure.

**Risk of data leakage from RCOG.** As hard copy documents are by nature written in unprotected, “clear text” format, unauthorised access is a significant risk. As such, confidential information should always be secured when unattended.

**Damage.** As paper files are susceptible to theft, fire and water damage, staff are encouraged to store information digitally where possible.

**Access restrictions**

**Public locations**

Access to RCOG confidential information should not be conducted from any location that is deemed to be a public environment e.g. coffee shop or train station. If accessing RCOG non-confidential information in a public place, care must be taken to ensure that the screen is not visible to any person who does not have a legitimate purpose for viewing the information. For more information, refer to the [Working from Home Policy](#).
Private locations

Remote access may be obtained from any location that has an internet connection and provides a secure location to connect without the risk of inadvertent disclosure of RCOG information; such areas include at home and hotel rooms and where there are no special requirements for remote access and existing broadband connections are acceptable.

General Access Guidelines

- Access to confidential information shall be restricted to authorised users who have a bona fide business need to access the information;
- Access rights to confidential information will be allocated by business area;
- Any additional access rights must be requested by the individual's line manager and agreed with the SIRO;
- Certain visitors and members shall have restricted access to the College network via workstations using restricted accounts. Approval for access will be required on an individual basis; and
- All other visitors and members will have access to certain restricted computers that are not part of the College network e.g. in the College library.

Security Measures

Personal and confidential data storage and use

- Personal and confidential data in either electronic or hard copy format, including that relating to members and patients, stored in a filing cabinet or on a RCOG laptop or mobile device should be kept to the minimum required for effective business use in order to minimise the risks and impacts of a breach.
- All personal and confidential information should be stored in a locked desk or filing cabinet. If in electronic format, it must be encrypted or stored in a restricted folder. Citrix must be used for remote access.
- Disc and file encryption products must be used correctly in accordance with instructions from the IT Team. In particular the password and any 2 factor authentication mechanism (if used) must be kept separate from the username and host device; these are effectively the encryption key. Separate file encryption or restricted folders should be used for items containing personal or confidential information. For guidance please contact the IT team.
- The impact of a breach of device security may therefore extend far more widely than the device itself.
- No user should use removable media to transfer any RCOG confidential information without the express permission of the IG Manager and without appropriate security measures in place.
• Personal or sensitive data should not be emailed to personal accounts, file upload sites or other cloud based data storage/transfer services under any circumstance without speaking to the IT Team first.

• Personal or sensitive data should not be transferred to personal computers, mobile devices or removed in hard copy form from RCOG offices without permission from the IG Manager.

• Any sensitive information stored on removable media should be encrypted using 7-Zip software. Encryption keys should be stored separately from the encrypted data.

• Any hardcopy information that contains personal or sensitive data must be sealed within two envelopes and sent by secure courier with a track and trace facility.

• Any bulk Information Sharing transactions will be subject to a Subject Specific or Purpose Specific Information Sharing agreement.

• Remote access to RCOG data and applications by staff shall be restricted to a Citrix portal. All staff should use the Citrix portal to log in remotely, and not transfer any information outside of this environment.

• All external contractors acting on behalf of the RCOG shall be required to ensure that confidential data is transferred securely, (encrypted data over an FTP or password protected). Passwords must not be provided alongside the confidential data i.e. in the same email

• If staff are transferring personal or confidential data outside of the organisation, they should seek advice from the IG Manager or IM&T teams.

**Physical**

Laptops, tablets or mobile devices, even when protected by disk encryption, should not be left in the care of any person who is not trusted to protect the information contained.

If left in the office overnight, they should be locked away or secured by a laptop lock.

File storage for paper files should always be locked when left unattended for any significant length of time. Offices will be locked overnight around 19:00 and opened again by the cleaners in the morning.

All external doors have keypad entry for access control. Offices containing personal and confidential material or assets (e.g. HR, archive store, exams scanning room, computer room) must have keypad security, with a separate code to common areas.

The RCOG building is secured every evening, with additional protection offered by 24/7/365 security/reception cover and CCTV. CCTV footage is stored digitally in the secure computer room and only authorised staff have access (IT/Ops).

Access to the computer room is only possible for authorised third party contractors or staff when accompanied by a member of the IT team.
Incident reporting

Unauthorized access to a secure area or loss or theft of RCOG laptops, tablets or mobile devices should be reported immediately to the police, RCOG Head of Information Management & Technology, the SIRO and IG Manager and also reported following RCOG’s IG Security Incident Reporting Procedure.

Secure disposal and reuse

Data stored on RCOG laptops should be securely erased before the laptop is reassigned for another person or disposed of when redundant. Failure to securely erase data may result in that data being available to the new owner/user. Therefore any RCOG laptop must be returned to the IT department for wiping and rebuilding before being reassigned.

Personal and confidential material in hard copy format must be disposed of using secure recycling bins.

Best practice

• Do not leave laptops/tablets/mobile devices unattended in car boots overnight;

• Do not leave laptops/tablets/mobile devices unattended in unsecure areas, for example meeting rooms next to areas of public access, and hotel rooms where others may have access. Make use of room locks and lockable storage facilities where available;

• Always use Citrix to access the RCOG network from remote locations;

• Be aware of the potential for opportunistic or targeted theft of laptop bags in busy public places including airports, train stations, hotel lobbies, exhibition halls etc. and on public transport e.g. buses and trains;

• Do not use laptops with removable media in places where that media could easily be left behind or misplaced;

• When travelling, avoid placing laptops in locations where they could be easily forgotten or left behind e.g. overhead racks and taxi boots;

• Be aware that the use of laptops in public places is likely to draw the attention of those in the vicinity. It is possible that information viewed on a laptop screen could lead to the unauthorized disclosure of that information;

• Particular care should be taken when closing the lid of the laptop. Hibernation should be enabled as a minimum although the user should be logged out as a preference. The user must be aware that whilst the laptop is turned on, encryption is NOT enabled as it is only effective when the laptop is turned off;
• Passwords should be at least 8 characters long, should contain a mixture of capital letters, numbers and non-standard characters, such as *, % or £. They will automatically require changing every 40 days and the same password cannot be used twice.

• Never provide a password alongside a password protected document i.e. in the same email

• Ensure digital copies of personal data are stored in restricted folders on the CFP

**Contracts of Employment**

The College will include clauses on confidentiality as standard in all contracts of employment.

Any additional staff security requirements shall be addressed at the recruitment stage.

**Security Control of Assets**

All IT hardware shall be recorded on an asset register and a security asset label should be placed on each asset.

Core IT hardware shall be held in secure locations and access restricted to authorised personnel.

No equipment shall be removed from the site without the prior approval of the Head of IM&T, except for portable computers and mobile devices that are the responsibility of each named individual user.

The server room shall be kept locked at all times and access shall be restricted to the IM&T and Buildings teams.

**Clinical Quality**

**Projects involving patient identifiable data**

All research projects should aim to comply with the Caldicott Principles in that:

• Every proposed use of patient identifiable information should be justified, defined and scrutinised.

• Patient identifiable information will only be used where there is no alternative.

• Only the minimum amount of patient identifiable information should be used in order to fulfil RCOG requirements.

• Access to patient identifiable information and associated systems will be controlled on a strict need to know basis.

• All staff handling patient identifiable information will undertake mandatory training on data security and protection, and may be asked to complete advanced training.
• All transfers and processes involving patient identifiable data (whether electronic or hard copy) will take place within the confines of the law, and where consent has not been explicitly obtained, appropriate Health Research Authority Confidentiality Advisory Group (section 251) approvals must be in place.

• Transfers of hard copy information that contain patient identifiable data should only be made in exceptional circumstances.

• Hardcopy information that contains sensitive patient identifiable data must be sealed within two envelopes and sent by secure courier with a track and trace facility.

Requesting remote access

Remote access via Citrix, outlook web access and the RCOG mobile app needs to be authorised by a departmental manager and is subject to review from time to time.

Direct integration with a mobile or tablet email client is allowed under special circumstances and subject to business justification and management approval. Provision of this service places specific security responsibilities on behalf of the user to meet Cyber Essentials Plus requirements. Specifically:

• at all times the mobile device should be maintained on a supported mainstream operating system
• evidence of the operating system software version must be maintained with the IMT service desk
• the user must maintain a pin number and ensure that the device is locked when not in use
• Synchronisation of calendar appointments is not supported due to the risk of counter corruption.
• Only the most recent 4 weeks of email will be available
• the user agrees not to copy or move emails or attachments to any personal storage, including the copying of such data in the form of device backups.
• the user will indemnify the college against any loss of personal data and understands that the College may delete the device (and possibly all data on the device) in order to remove College emails if required.
• access authorisation will be reviewed periodically

If remote access was not provided as part of the initial user setup procedure it can be requested at a later stage by using the “remote access request form” on the Internet.

Procurement of Information Systems and Change Control

No new information system, hardware, software or removable media should be purchased or installed without IM&T approval.
All changes to information systems, application or networks shall be reviewed and approved by the Head of IM&T.

**Systems Monitoring**

All IT activities on RCOG IT equipment that include hardware and software can be monitored but only in compliance with RCOG’s data protection policy.

**Information Security Training**

Data security and protection online training is mandatory for all members of staff and included as part of the induction process.

An ongoing awareness programme and refresher training sessions is maintained to ensure that staff awareness is up to date.

| VERSION CONTROL |
|-----------------|--------------------|----------------|-------------------|
| Author:         | Director of IM&T   | Version:       | 0.3               |
| Creation Date:  | September 2016     | Last review date: | 15 March 2019 |
| Signed off by:  | IGMG               | Sign off Date:  | 29 March 2019    |
Appendix A – Legislative Framework

The RCOG is obliged to abide by all relevant UK and European Union legislation. This requirement to comply with the legislation shall be devolved to employees, who will be held personally responsible for any breaches of security for which they are accountable.

The RCOG aims to comply with the following where appropriate:

- International standard on Records Management (ISO15489)
- General Data Protection Regulation (GDPR) 2016 and the UK Data Protection Act 2018
- International Standard on Information Security (ISO27001)
- British standard on legal admissibility and evidential weight of information stored electronically (BS10008)
- NHS Information Governance Framework
- Copyright, Designs and Patents Act 1990
- Computer Misuse Act 1990
- Human Rights Act 1998
- Criminal Justice Act 1988