Information Security Policy for Associates and Contractors

Version: 1.17  
Status: Issued  
Date: 24 November 2021  
Reference: 88339411  
Review cycle: Annual
Introduction

Purpose

1 This guidance outlines your responsibilities as a GMC associate or contractor when handling sensitive information which comes into your possession whilst carrying out your role for the GMC, MPTS or GMCSI. This may be provided to you by contacts who are not GMC, MPTS or GMCSI employees. Contractors and associates include, for example: Education visitors, performance assessors, health assessors, panellists. All GMC, MPTS or GMCSI information is considered to be sensitive unless it is known to be in the public domain.
Scope

2 This document defines how associates, contractors and any authorised individual who is a subcontractor (eg secretary) with a contractual duty of confidence to the associate or contractor should process, store, transfer and dispose of GMC, MPTS or GMCSI confidential information.

3 While working on behalf of the GMC, MPTS or GMCSI you will be given access to sensitive information. This may include data about living, identifiable individuals, information about internal policy discussions, commercially sensitive data and any other information concerning GMC, MPTS or GMCSI or third party business that is not in the public domain.

4 Personal data about individuals must be processed in compliance with data protection legislation and the GMC’s data protection and information security policies.

Responsibilities

5 The Head of Information Security and Records Management shall ensure that this procedure is up-to-date and relevant.

6 GMC, MPTS and GMCSI section heads must take reasonable steps to ensure their contractors and associates comply with this policy.

7 Associates and contractors must comply with this policy or their contract may be terminated.

Related Procedures

- GMC Data Protection Policy
- GMC Information Security Policy

Reference Documentation

None.

Guidelines

Overview

8 Sensitive information must not be divulged to anyone outside the GMC, MPTS or GMCSI unless this is required by law or you have authorisation to do so. It is
therefore necessary that you take precautions against accidental disclosure and follow security procedures at all times. You should always be aware of the location of information that you have been provided with. Always make sure that it is secure and not accessible to unauthorised individuals. An example of an authorised individual is a subcontractor (eg. secretary) with a contractual duty of confidence to the contractor and/or the GMC, MPTS or GMCSI.

Handling information

9  Be aware of your environment and do not work on documents containing personal data or sensitive information in public places where other people may be able to read what you are viewing (eg on a train). Use a laptop privacy screen if necessary.

10  Do not make phone calls in public where you may be discussing or asking for personal data about any individuals or exchanging other confidential information.

11  Do not discuss sensitive GMC, MPTS or GMCSI information with anyone outside the GMC, MPTS or GMCSI, unless this is required by law or you have authorisation to do so.

12  Do not discuss sensitive GMC information in public areas or in break out areas on GMC or MPTS premises.

13  Do not view, or open GMC, MPTS or GMCSI information on a publicly accessible computer (for example in a public library or internet café).

14  When transporting GMC, MPTS or GMCSI records, they must be kept with you at all times and secured appropriately, eg using a suitable bag lock.

Storing information

15  Keep information orderly and in a format from which data can easily be retrieved.

16  Make sure papers are stored in proper files and not in unordered bundles where information could be easily lost.

17  Papers must be stored securely when not in use, eg in a locked desk or cabinet.

a  Do not use third party web-based applications or file sharing systems for the storage, sharing or processing of GMC, MPTS or GMCSI material. Examples include Dropbox and iCloud.
b Do not store GMC, MPTS or GMCSI information on an unencrypted USB memory stick. If you need to store information on a USB memory stick, please speak to your contact and they can arrange for you to be provided with a GMC encrypted USB memory stick.

c Avoid using a shared home computer, laptop or tablet to perform GMC business. If this is not possible, you must ensure that any sensitive information is stored in a secure encrypted folder or a password controlled area on an encrypted device so that only you can access this information.

Transferring information

18 Do not transfer data onto portable media such as non-GMC memory sticks, CDs or DVDs.

19 The GMC and MPTS provide two systems to allow sensitive information to be exchanged electronically and securely over the internet. They are known as GMC Connect (Connect if you work with the MPTS) and SFTS. Each has a different purpose. You will be given guidance and/or training if your interactions with us involve using one of these systems. If you are a user of one of these systems do not access them on a shared or publicly accessible computer. You may also be given instruction not to make printed copies of electronic data shared with you.

Depending on your browser, it’s likely that viewing documents in GMC Connect will lead to a temporary copy being downloaded to your device. Make sure you delete your temp files on a scheduled basis. There’s guidance available online explaining how to do this as it depends on which operating system and version you’re using.

20 We may transfer confidential records to you using an encrypted USB memory stick. You must not transfer data from this device onto your computer’s hard drive or any other storage medium.

a If you are provided with an encrypted memory stick by the GMC, you will be given a password by your GMC, MPTS or GMCSI contact. You must keep this secure and you must not divulge the password to anyone.

b If you are provided with an encrypted memory stick by the GMC, when you create new documents, you must only store these on the GMC memory stick. Do not create documents on your computer’s hard drive. Only GMC, MPTS or GMCSI documents shall be stored on the memory stick to reduce the risk of virus infection.
On completion of a particular assignment of work, the encrypted memory stick must be returned to your GMC, MPTS or GMCSI contact.

Disposing of information

21 Once GMC, MPTS or GMCSI information is no longer needed, e.g. because a piece of work has been concluded or your involvement with us ceases, please return the information (and/or encrypted memory stick) to us in the manner prescribed by your GMC, MPTS or GMCSI contact or dispose of the information in a secure manner. Your contact will be able to advise on secure disposal.

Technology

General password management best practice

22 When setting up a password on any system or device that you use to access sensitive information, it is best practice not to use a password or derivative (eg. myusualpassword1 or myusualpassword2) of a password you have previously used or currently use for your own personal online accounts.

23 Never share or write down your password and if you suspect it has been compromised, make sure you change it immediately.

24 Do not use the same password for different systems. Always make sure each individual system has a unique password. This helps to avoid passwords being compromised on multiple systems if only one is affected. There is some advice on password good practice here: [https://www.getsafeonline.org/protecting-yourself/passwords/](https://www.getsafeonline.org/protecting-yourself/passwords/)

Securing your home broadband router

25 Most home broadband is delivered through a router supplied by your broadband service provider. The router is the box that plugs into your home phone line socket. You connect to the router by either a network cable or, more commonly, by a wireless (WiFi) connection in order to access the internet.

26 Your router will usually have been supplied with two passwords; one to connect to the WiFi network, and the other giving you access to change the configuration of your router. These are usually printed on a label underneath, or on the back of your router.
27 In some cases, the default 'admin' passwords are publicly available on the internet so we strongly recommend you change your router password from the one given to you by your internet service provider in order to help keep your network secure.

**Changing your router's password**

28 To change the password, you should follow the instructions provided by your service provider. These are often provided on their website or through their customer services.

29 For maximum security, we recommend that you change the default password to one that contains:

   a uppercase and lowercase letters

   b numbers, and

   c non-alphabetic characters (like #, &, %, £)

30 This will ensure that only you have access to use your internet connection and nobody can change the configuration of your router without your knowledge.

31 Your router will probably need to restart in order to change the password.

**If you use a laptop for GMC, MPTS or GMCSI business:**

32 GMC, MPTS or GMCSI data must be stored in an encrypted format. The hard disk must be encrypted.

33 Where full disk encryption is not practical, we recommend using either:

   a The file encryption feature in Windows, where you can choose to encrypt selected files.

   b Folder encryption such as a native Mac encrypted folder.

   c A GMC encrypted USB key, which you can request from your contact.

34 It must be kept physically secured or with you at all times.

35 It must have appropriate password security applied to avoid the risk of unauthorised individuals gaining access to confidential information. Our secure password requirements are as follows:
a  At least 8 characters long 

b  Must not contain your account or full name 

c  Contain at least three of the following four character groups:
   - English uppercase characters (A through Z)
   - English lowercase characters (a through z)
   - Numerals (0 through 9)
   - Non-alphabetic characters (such as £, %, &)

Your computer and/or laptop must contain anti-virus software. You must keep this software up to date.

If you use an iPad for GMC, MPTS or GMCSI business:
   a  You must keep the operating system up to date in line with Apple’s recommendations.

   b  You must have a passcode enabled to ensure the iPad is encrypted.

   c  It must be kept physically secured or with you at all times.

   d  Local wipe and remote wipe must be enabled.

36  It must have appropriate password security applied to avoid the risk of unauthorised individuals gaining access to confidential information. Native Apple facial recognition password security is acceptable.

37  For those contractors who use Dictaphones to undertake GMC, MPTS or GMCSI work, we recommend the use of 256-bit AES encrypted and password protected devices and storing the recording on the device, rather than a removable SD memory card.

Information Security and Data Protection Breaches

38  We have a collective responsibility to ensure that the confidentiality and security of our information is maintained. Occasionally things can go wrong. You must report data protection breaches involving our information immediately to your contact at the GMC, MPTS or GMCSI.

39  When reporting the breach or incident, please provide as much information as possible, eg. what did you see, what was disclosed, when did it occur, who was involved, where did it happen, what is the potential impact? This will enable us to
effectively deal with the incident or breach. For example, if you discover unattended GMC, MPTS or GMCSI material in the course of your duties, in any format, please notify a member of our staff immediately.

**Homeworking FAQ’s**

During the pandemic many of us are required to work from home and have had to change the way we work. Our associates and contractors all work in different ways, providing a number of different services for the GMC, MPTS and GMCSI.

Not all of the questions below will be relevant to your specific role and if you have any questions or need further clarification, please direct them to your GMC, MPTS or GMCSI contact.

40 **I need to take notes to perform my role. Normally I’d take my used notebooks into work, or into the GMC or MPTS to get them securely shredded. What should I do with them?**

You should record notes electronically wherever possible, saving them to a secure area where they can be deleted after use. If you do need to make paper notes, you must ensure there’s no personal or sensitive information written down. Don’t put any GMC, MPTS or GMCSI documents or sensitive information in your household waste.

If you have personal or sensitive information in notebooks already, keep them secure, for example in a locked cabinet or laptop bag until you can return them to your workplace or GMC / MPTS offices to put them in the confidential waste bins for secure shredding after use.

If you wish to use your own shredding device at home, that’s fine too but you’ll need to check that it cross cut shreds to P-4 size as defined in the confidential shredding standard DIN 66399 where P-7 is the most secure and P-1 is the least secure – most shredders have the P rating listed as part of the product specification online.

41 **I live in a shared house and it’s not possible for me to work in a separate room. Should I be using a privacy screen whilst working at home?**

If people in your household can easily see what you’re working on, then you should be using a privacy screen for your laptop.

Privacy screens for larger monitors are expensive so before making a purchase, we’d recommend you firstly assess if you could do any confidential work using your laptop with a privacy screen on it.
If you work with sensitive personal information on your screen for a significant proportion of the day and using your laptop screen isn’t practical, you should explore other ways to physically shield your monitor screen from others in your household. Could you move position so your monitor faces towards a wall or faces away from where people enter the room or walk behind you? If none of this is possible, you should consider purchasing a monitor privacy screen. Unfortunately the GMC / MPTS won't be able to reimburse you for the cost of a privacy screen.

42 **There are more distractions at home and I'm finding it hard to concentrate, I feel I'm more at risk of causing a disclosure incident. How can I reduce the risk?**

Working from home in a busy household can be challenging. Loss of concentration is a common cause of disclosure incidents and the following basic tips can help you avoid this:

- **Stop, check, then send.** Take time to check what you’re sending is correct before you send it. Is that definitely the right email address and are those definitely the right attachments?

- **If you’re sending something late in the day/evening, is it better to wait until the morning to have a quick, fresh look at it?**

- **Make time for regular screen breaks to give yourself a rest**

43 **Am I ok to use my home printer to print out GMC, MPTS or GMCSI information?**

For many Associate and contractor roles, we discourage home printing as it invariably presents more risk of accidental disclosure and the issue of how to then securely destroy the documents after use. If your GMC, MPTS or GMCSI contact has advised that we do need you to print papers on your home printer, we’ve provided a security checklist for you to follow:

- **For wireless and bluetooth printers, make sure you have changed the default password for your printer (this can be found within the security or utility settings on your printer.)**

- **When the manufacturer issues firmware updates for your printer, apply these as soon as possible - these updates will address any new security vulnerabilities.**

- **Keep printed papers secure eg. in a locked cabinet or locked laptop bag.**

- **Securely destroy any printed papers after use and do not dispose of them in household waste unless they have been securely shredded to P-4 size first.**
44 I deal with sensitive information as part of my role, what is the position on the use of headsets?

Wherever possible, you should always use a headset when making and accepting calls and attending meetings to keep the information the caller is providing private. If you live with others, try to make sure your calls cannot be overheard wherever possible.

Headsets also improve the audio quality in calls and meetings for you and the other participants.

If there’s a specific reason why using a headset isn’t practical for you and you deal with sensitive calls as part of your role, please discuss this further with your GMC, MPTS, GMCSI contact so you can agree ways to minimise the risk.

45 I’ve received a suspicious email. What should I do?

Phishing and malicious email attacks are becoming increasingly sophisticated and common so it’s important we’re all vigilant. If you receive an email that doesn’t seem right, you should do the following*:

- Don’t open any links or attachments
- If it looks like it’s been sent from someone at the GMC, MPTS or GMCSI, don’t forward us the email initially, please contact us and we’ll provide guidance.
- After it’s been investigated, delete the email from your mailbox and from your deleted items (hard delete – SHIFT + Delete)

*If you work within the NHS or another organisation then you should follow the guidance they’ve provided.

Further advice

46 If you have any questions about this policy, please direct these to your GMC, MPTS or GMCSI contact in the first instance.

47 For further information on recommended password security, anti-virus and encryption software, you can visit Get Safe Online at www.getsafeonline.org/